

# HP Data Protector 6.20

## guide conceptuel

Référence:  
Première Édition: Mars 2011



## Informations juridiques

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

Logiciel informatique confidentiel. Licence HP valide requise pour la possession, l'utilisation ou la copie. Conformément aux directives FAR 12.211 et 12.212, les logiciels informatiques commerciaux, ainsi que la documentation et les données techniques associées, sont concédés à l'Administration américaine dans le cadre de la licence commerciale standard du fournisseur.

Les informations fournies dans le présent document sont susceptibles d'être modifiées sans préavis. Les seules garanties applicables aux produits et services HP sont énoncées dans les déclarations de garantie expresse accompagnant lesdits produits et services. Aucune information du présent document ne saurait être considérée comme constituant une garantie supplémentaire. HP ne saurait être tenue pour responsable des éventuelles omissions ou erreurs techniques et éditoriales 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 d'Oracle Corporation, Redwood City, Californie.

UNIX® est une marque déposée de The Open Group.

---

# Sommaire

Historique des publications .....	19
A propos de ce manuel .....	21
Public visé .....	21
Documentation .....	21
Guides .....	21
Aide en ligne .....	25
Organisation de la documentation .....	25
Abréviations .....	25
Organisation .....	27
Intégrations .....	27
Conventions typographiques et symboles .....	29
Interface utilisateur graphique de Data Protector .....	30
Informations générales .....	30
Assistance technique HP .....	31
Service d'enregistrement .....	31
Sites Web HP : .....	31
Vos commentaires sur la documentation .....	31
1 A propos de la sauvegarde et de Data Protector .....	33
Dans ce chapitre .....	33
A propos de Data Protector .....	33
Présentation des sauvegardes et des restaurations .....	37
Qu'est-ce qu'une sauvegarde ? .....	37
Qu'est-ce qu'une restauration ? .....	38
Sauvegarde d'un environnement réseau .....	38
Architecture de Data Protector .....	39
Opérations effectuées dans la cellule .....	41
Sessions de sauvegarde .....	42
Sessions de restauration .....	43
Environnements d'entreprise .....	44
Séparation d'un environnement en plusieurs cellules .....	45
Gestion des supports .....	48

Périphériques de sauvegarde .....	49
Interfaces utilisateur .....	50
Interface utilisateur graphique de Data Protector .....	51
Interface graphique Java de Data Protector .....	52
Présentation des tâches nécessaires à la configuration de Data Protector .....	55
<b>2 Planification de la stratégie de sauvegarde .....</b>	<b>57</b>
Dans ce chapitre .....	57
Planification d'une stratégie de sauvegarde .....	58
Définition des besoins relatifs à une stratégie de sauvegarde .....	58
Facteurs influant sur votre stratégie de sauvegarde .....	61
Préparation d'un plan de stratégie de sauvegarde .....	61
Planification de cellules .....	63
Une ou plusieurs cellules ? .....	63
Installation et maintenance des systèmes client .....	65
Création de cellules dans l'environnement UNIX .....	66
Création de cellules dans l'environnement Windows .....	66
Domaines Windows .....	66
Groupes de travail Windows .....	67
Création de cellules dans un environnement mixte .....	67
Cellules distantes géographiquement .....	68
Analyse et planification des performances .....	69
Infrastructure .....	69
Sauvegarde locale ou réseau .....	69
Périphériques .....	69
Matériel hautes performances autre que les périphériques .....	70
Configuration hautes performances avancée .....	70
Utilisation en parallèle du matériel .....	71
Configuration des sauvegardes et des restaurations .....	72
Compression logicielle .....	72
Compression matérielle .....	72
Sauvegardes complètes et incrémentales .....	72
Sauvegarde d'image disque ou sauvegarde de système de fichiers .....	73
Distribution des objets sur les supports .....	73
Performances des disques .....	74
Performances SAN .....	75
Performances des applications de base de données en ligne .....	75
Planification de la sécurité .....	76
Cellules .....	76
Comptes utilisateur Data Protector .....	77
Groupes d'utilisateurs Data Protector .....	77
Droits utilisateur Data Protector .....	78

Visibilité des données sauvegardées .....	78
Qu'est-ce que la propriété de sauvegarde ? .....	79
Cryptage des données .....	79
Fonctionnement du cryptage AES 256 bits de Data Protector .....	80
Fonctionnement du cryptage sur lecteur de Data Protector .....	81
Restauration à partir de sauvegardes cryptées .....	82
Communications de contrôle cryptées .....	82
Fonctionnement des communications de contrôle cryptées dans Data Protector .....	83
Cryptage des données et communications de contrôle cryptées .....	84
Gestion de clusters .....	85
Concepts rattachés aux clusters .....	85
Support de clusters .....	88
Exemples d'environnements de clusters .....	89
Gestionnaire de cellule installé hors d'un cluster .....	89
Gestionnaire de cellule installé hors d'un cluster, périphériques connectés aux nœuds de cluster .....	91
Gestionnaire de cellule installé dans un cluster, périphériques connectés aux nœuds de cluster .....	94
Sauvegardes complètes et incrémentales .....	98
Sauvegardes complètes .....	99
Sauvegarde synthétique .....	99
Sauvegardes incrémentales .....	99
Sauvegarde incrémentale classique .....	99
Sauvegarde incrémentale avancée .....	100
Sauvegarde incrémentale au moyen du module fournisseur d'informations sur les modifications .....	100
Types de sauvegardes incrémentales .....	101
Observations relatives à la restauration .....	103
Conservation des données sauvegardées et des informations sur les données .....	106
Protection des données .....	107
Protection de catalogue .....	107
Niveau de journalisation .....	108
Exploration des fichiers à restaurer .....	108
Activation de l'exploration des fichiers et de la restauration rapide .....	108
Activation de la restauration des fichiers, sans l'exploration .....	109
Ecrasement des fichiers sauvegardés par de nouvelles données .....	109
Exportation de supports d'une cellule .....	109
Sauvegarde de données .....	110
Création d'une spécification de sauvegarde .....	111
Sélection d'objets sauvegarde .....	111
Sessions de sauvegarde .....	113
Miroirs d'objet .....	113

Jeux de supports .....	114
Types de sauvegarde et sauvegardes planifiées .....	114
Planification, configurations et sessions de sauvegarde .....	114
Planification - Conseils et pièges à éviter .....	115
Quand planifier des sauvegardes ? .....	115
Planification échelonnée de sauvegardes complètes .....	116
Optimisation de la restauration .....	116
Opération automatisée ou sans surveillance .....	119
A propos des sauvegardes sans surveillance .....	120
Duplication de données sauvegardées .....	121
Copie d'objets .....	123
Pourquoi utiliser la fonction de copie d'objet ? .....	126
Mise en miroir d'objets .....	130
Copie de supports .....	133
Copie automatisée des supports .....	135
Copie intelligente de supports avec VLS .....	135
Vérification des supports et des objets de sauvegarde .....	136
Qu'est-ce que la vérification de support ? .....	136
Que vous apporte la vérification de supports ? .....	137
Qu'est-ce que la vérification d'objets ? .....	137
Que vous apporte la vérification d'objets ? .....	137
Restauration des données .....	138
Durée de la restauration .....	138
Sélection du jeu de supports .....	139
Sélection des périphériques .....	140
Opérateurs autorisés à restaurer les données .....	141
Utilisateurs finaux autorisés à restaurer les données .....	142
Récupération après sinistre .....	143
Méthodes de récupération après sinistre .....	144
Autres méthodes de récupération après sinistre .....	145

### 3 Gestion des supports et périphériques ..... 147

Dans ce chapitre .....	147
Gestion des supports .....	147
Cycle de vie des supports .....	149
Pools de supports .....	150
Pools libres .....	152
Pools de supports, exemples d'utilisation .....	155
Mise en œuvre d'une stratégie de rotation des supports .....	158
Rotation des supports et Data Protector .....	159
Supports requis pour la rotation .....	159
Gestion des supports avant le début des sauvegardes .....	160

Initialisation ou formatage des supports .....	160
Étiquetage des supports Data Protector .....	161
Champ Emplacement .....	161
Gestion des supports pendant une session de sauvegarde .....	162
Sélection des supports utilisés pour la sauvegarde .....	163
Ajout de données aux supports pendant des sessions de sauvegarde .....	163
Écriture de données sur plusieurs jeux de supports pendant la sauvegarde .....	166
Détermination de l'état des supports .....	166
Gestion des supports après une session de sauvegarde .....	167
Mise au coffre .....	168
Restauration à partir de supports stockés dans un coffre .....	169
Périphériques .....	170
Listes de périphériques et partage de charge .....	172
Fonctionnement du partage de charge .....	173
Périphérique en mode continu et simultanéité .....	173
Taille de segment .....	175
Taille de bloc .....	176
Nombre de mémoires tampon utilisées par les Agents de disque .....	176
Verrouillage de périphérique et noms de verrouillage .....	177
Périphériques autonomes .....	178
Petits périphériques de magasin .....	179
Grandes bibliothèques .....	179
Gestion des supports .....	180
Taille d'une bibliothèque .....	180
Partage d'une bibliothèque avec d'autres applications .....	181
Logements d'insertion/d'éjection .....	181
Prise en charge des codes-barres .....	181
Prise en charge des bandes nettoyantes .....	182
Partage d'une bibliothèque entre plusieurs systèmes .....	183
Data Protector et réseaux SAN .....	189
Storage Area Networks .....	189
Fibre Channel .....	190
Topologie point à point .....	191
Topologie en boucle .....	191
Topologie commutée .....	192
Partage de périphériques dans un SAN .....	193
Configuration de plusieurs chemins vers des périphériques physiques .....	193
Verrouillage de périphérique .....	195
Accès direct et indirect à la bibliothèque .....	196
Accès indirect à la bibliothèque .....	196
Accès direct à la bibliothèque .....	197
Partage de périphériques dans les clusters .....	198
Lecteurs statiques .....	198

Lecteurs flottants .....	199
--------------------------	-----

## 4 Utilisateurs et groupes d'utilisateurs ..... 201

Dans ce chapitre .....	201
Sécurité renforcée pour les utilisateurs Data Protector .....	201
Accès à des données sauvegardées .....	201
Utilisateurs et groupes d'utilisateurs .....	202
Utilisation des groupes d'utilisateurs prédéfinis .....	203
Droits utilisateur Data Protector .....	204

## 5 Base de données interne de Data Protector ..... 205

Dans ce chapitre .....	205
A propos de la base de données IDB .....	205
Base de données IDB dans le Gestionnaire de cellule Windows .....	206
Base de données IDB dans le Gestionnaire de cellule UNIX .....	207
Base de données IDB dans un environnement Manager-of-Managers .....	207
Architecture de la base de données IDB .....	207
Base de données de gestion des supports (MMDB) .....	209
Base de données catalogue (CDB) .....	210
Fichiers binaires de catalogue des détails (DCBF) .....	211
Fichiers binaires de messages de session (SMBF) .....	212
Fichiers binaires d'intégrations sans serveur (SIBF) .....	213
Banque de clés de cryptage et fichiers catalogue .....	214
Fonctionnement de la base de données IDB .....	215
Pendant la sauvegarde .....	215
Pendant la restauration .....	215
Pendant la copie ou la consolidation d'objets .....	216
Pendant la vérification d'objet .....	216
Exportation de supports .....	217
Suppression du catalogue des détails .....	217
Purge des noms de fichier .....	218
Purge des versions de fichier .....	218
Présentation de la gestion de la base de données IDB .....	218
Croissance et performances de la base de données IDB .....	219
Facteurs clés des performances et de la croissance de l'IDB .....	219
Croissance et performances de la base de données IDB : paramètres clés réglables .....	220
Niveau de journalisation comme paramètre clé réglable de l'IDB .....	221
Protection de catalogue comme paramètre clé réglable de l'IDB .....	223
Utilisation recommandée du niveau de journalisation et de la protection de catalogue .....	224
Estimation de la taille de l'IDB .....	226



<b>6 Gestion des services .....</b>	<b>227</b>
Dans ce chapitre .....	227
Généralités .....	227
Data Protector et la gestion des services .....	228
Fonctionnalité Data Protector native .....	228
Application Response Measurement version 2.0 (API ARM 2.0) .....	230
Intégration avec le logiciel HP Operations Manager .....	231
Interruptions SNMP .....	231
Moniteur .....	232
Génération de rapports et notification .....	232
Journalisation et notification des événements .....	234
Fichiers journaux Data Protector .....	234
Journal de l'application Windows .....	235
Rapports Java en ligne .....	235
Mécanisme de vérification et de maintenance Data Protector .....	235
Gestion centralisée, environnement distribué .....	236
Utilisation des données fournies par Data Protector .....	236
<b>7 Fonctionnement de Data Protector .....</b>	<b>237</b>
Dans ce chapitre .....	237
Processus ou services Data Protector .....	237
Sessions de sauvegarde .....	239
Sessions de sauvegarde interactives ou planifiées .....	239
Flux de données et processus d'une session de sauvegarde .....	239
Commandes pré-exécution et post-exécution .....	242
Mise en attente des sessions de sauvegarde .....	243
Demandes de montage au cours d'une session de sauvegarde .....	243
Sauvegarde en mode détection de disques .....	244
Sessions de restauration .....	245
Flux de données et processus d'une session de restauration .....	245
Mise en attente des sessions de restauration .....	246
Demandes de montage au cours d'une session de restauration .....	247
Restaurations parallèles .....	247
Restauration multiple et rapide de fichier unique .....	248
Reprise des sessions de restauration .....	249
Session de copie d'objet .....	249
Sessions de copie d'objet automatique et interactive .....	249
Flux de données et processus d'une session de copie d'objet .....	250
Mise en attente des sessions de copie d'objet .....	252
Demandes de montage dans une session de copie d'objet .....	252
Sessions de consolidation d'objet .....	253
Sessions de consolidation d'objet automatique et interactive .....	253

Flux de données et processus d'une session de consolidation d'objet .....	254
Mise en attente des sessions de consolidation d'objet .....	255
Demandes de montage dans une session de consolidation d'objet .....	255
Sessions de vérification d'objet .....	256
Sessions de vérification d'objet automatiques et interactives .....	256
Flux de données et processus d'une session de vérification d'objet .....	257
Sessions de gestion des supports .....	258
Flux de données d'une session de gestion des supports .....	258
<b>8 Intégration avec des applications .....</b>	<b>261</b>
Intégration aux applications de base de données .....	261
Présentation d'une base de données .....	261
Sauvegarde de systèmes de fichiers de bases de données et d'applications .....	263
Sauvegarde en ligne de bases de données et d'applications .....	264
Intégration avec les environnements de virtualisation .....	266
Sauvegarde hors ligne du système de fichiers des machines virtuelles .....	266
Sauvegarde en ligne de machines virtuelles .....	267
<b>9 Sauvegarde sur disque .....</b>	<b>269</b>
Dans ce chapitre .....	269
Généralités .....	269
Avantages de la sauvegarde sur disque .....	270
Périphériques sur disque Data Protector .....	271
<b>10 Sauvegarde synthétique .....</b>	<b>275</b>
Dans ce chapitre .....	275
Généralités .....	275
Avantages de la sauvegarde synthétique .....	276
Fonctionnement de la sauvegarde synthétique Data Protector .....	276
Sauvegarde synthétique et utilisation d'espace de support .....	278
Sauvegarde synthétique et restauration .....	278
Influence des périodes de protection des données sur la restauration à partir d'une sauvegarde synthétique .....	281
<b>11 Concepts Split Mirror .....</b>	<b>283</b>
Dans ce chapitre .....	283
Généralités .....	283
Configurations prises en charge .....	287
Miroir local - hôte double .....	287
Miroir local - hôte simple .....	289
Miroir distant .....	289

Combinaison de miroirs local et distant .....	291
Autres configurations .....	292
<b>12 Concepts de snapshot .....</b>	<b>295</b>
Dans ce chapitre .....	295
Généralités .....	295
Virtualisation du stockage .....	295
Concepts de snapshot .....	296
Types de sauvegardes de snapshot .....	298
Restauration instantanée .....	299
Jeu de répliques et rotation d'un jeu de répliques .....	299
Types de snapshots .....	300
Configurations prises en charge .....	301
Configuration de base : baie de disques simple - hôte double .....	301
Autres configurations prises en charge .....	303
Autres configurations .....	305
<b>13 Microsoft Volume Shadow Copy Service .....</b>	<b>307</b>
Dans ce chapitre .....	307
Généralités .....	307
Intégration de Data Protector à Volume Shadow Copy Service .....	312
Sauvegarde et restauration de système de fichiers VSS .....	313
<b>A Scénarios de sauvegarde .....</b>	<b>317</b>
Dans cette annexe .....	317
Éléments à prendre en considération .....	317
Entreprise XYZ .....	319
Environnement .....	319
Besoins relatifs à une stratégie de sauvegarde .....	322
Solution proposée .....	323
Entreprise ABC .....	335
Environnement .....	335
Besoins relatifs à une stratégie de sauvegarde .....	337
Solution proposée .....	340
<b>B Informations complémentaires .....</b>	<b>355</b>
Dans cette annexe .....	355
Généralités de sauvegarde .....	355
Exemples de copie automatisée des supports .....	356
Exemple 1 : copie automatisée des supports de sauvegarde de systèmes de fichiers .....	357

Sauvegarde Incr1 .....	358
Sauvegarde complète .....	360
Exemple 2 : copie automatisée des supports de sauvegardes de base de données	
Oracle .....	363
Sauvegarde complète .....	364
Internationalisation .....	365
Localisation .....	365
Gestion des noms de fichier .....	366
Quelques explications .....	366
Gestion des noms de fichier lors d'une sauvegarde .....	367
Exploration des noms de fichier .....	367
Gestion des noms de fichier lors d'une restauration .....	368
 Glossaire .....	 369
 Index .....	 439

---

# Figures

1 Interface utilisateur graphique de Data Protector .....	30
2 Processus de sauvegarde .....	38
3 Processus de restauration .....	38
4 Sauvegarde réseau .....	39
5 Cellule Data Protector (description physique et logique) .....	40
6 Opération de sauvegarde ou de restauration .....	42
7 Session de sauvegarde .....	43
8 Session de restauration .....	44
9 Environnement d'entreprise Data Protector étendu .....	45
10 Gestion centralisée de plusieurs cellules .....	46
11 Environnement Manager-of-Managers .....	47
12 Liens entre les spécifications de sauvegarde, les périphériques et les pools de supports .....	49
13 Utilisation de l'interface utilisateur de Data Protector .....	51
14 Interface graphique Data Protector d'origine .....	52
15 interface graphique Java de Data Protector .....	52
16 Architecture de l'interface graphique Java de Data Protector .....	53
17 Session de sauvegarde avec cryptage AES 256 bits .....	81
18 Session de sauvegarde avec cryptage AES 256 bits et cryptage sur lecteur .....	82
19 Communications de contrôle cryptées .....	84
20 Communications de contrôle cryptées et cryptage des données .....	85
21 Structure d'un cluster type .....	86
22 Gestionnaire de cellule installé hors d'un cluster .....	90

23	Gestionnaire de cellule installé hors d'un cluster, périphériques connectés aux nœuds de cluster .....	92
24	Gestionnaire de cellule installé dans un cluster, périphériques connectés aux nœuds de cluster .....	95
25	Sauvegardes incrémentales .....	102
26	Sauvegardes incrémentales par niveau .....	102
27	Supports nécessaires à la restauration à partir de sauvegardes incrémentales simples et par niveau .....	105
28	Supports nécessaires à la restauration à partir de sauvegardes incrémentales par niveau .....	105
29	Session de sauvegarde .....	110
30	Sauvegarde complète avec des sauvegardes incrémentales simples quotidiennes .....	117
31	Sauvegarde complète avec des sauvegardes incrémentales quotidiennes de niveau 1 .....	118
32	Sauvegarde complète avec des sauvegardes incrémentales mixtes .....	119
33	Concept de la copie d'objet .....	123
34	Libération de supports .....	127
35	Démultiplexage d'un support .....	128
36	Concept de sauvegarde de disque en plusieurs étapes .....	129
37	Mise en miroir d'objets .....	132
38	Pools libres .....	153
39	Relation simple entre un périphérique et un pool de supports .....	155
40	Configuration des pools de supports pour les grandes bibliothèques ....	156
41	Périphériques multiples, pool de supports unique .....	157
42	Périphériques multiples, pools de supports multiples .....	158
43	Plusieurs objets et sessions par support, écritures séquentielles .....	164
44	Plusieurs objets et sessions par support, écritures simultanées .....	165
45	Plusieurs supports par session et par objet .....	165
46	Chaque objet est écrit sur un support séparé .....	166
47	Format de données .....	175

48	Verrouillage de périphérique et noms de périphérique .....	178
49	Connexion de lecteurs à plusieurs systèmes .....	183
50	Partage d'une bibliothèque SCSI (robot relié à un système client Data Protector) .....	186
51	Partage d'une bibliothèque SCSI (robot relié à un serveur NDMP) .....	187
52	Partage d'une bibliothèque ADIC/GRAU ou StorageTek ACS .....	188
53	Storage Area Network .....	190
54	Protocole LIP (Loop Initialization Protocol) .....	192
55	Exemple de configuration multichemins .....	194
56	Accès indirect à la bibliothèque .....	197
57	Accès direct à la bibliothèque .....	198
58	Parties de l'IDB .....	209
59	Influence du niveau de journalisation et de la protection de catalogue sur la croissance de la base de données IDB .....	221
60	Flux de données de la session de sauvegarde (1) .....	241
61	Flux de données d'une session de sauvegarde - sessions multiples .....	242
62	Flux de données d'une session de restauration .....	246
63	Flux de session d'une restauration parallèle .....	248
64	Flux de données d'une session de copie d'objet .....	252
65	Base de données relationnelle .....	262
66	Intégration de Data Protector à des bases de données .....	265
67	Sauvegarde synthétique .....	277
68	La sauvegarde complète virtuelle .....	278
69	Sauvegardes complètes et incrémentales .....	279
70	Sauvegarde synthétique .....	279
71	Sauvegarde synthétique régulière .....	280
72	Sauvegarde synthétique et copie d'objet .....	280
73	Concept de la sauvegarde Split Mirror .....	284
74	Miroir local - hôte double (sauvegarde avec performances optimales et temps d'indisponibilité nul) .....	288

75	Split Mirror - miroir distant (sauvegarde distante indépendante du réseau local - données haute disponibilité) .....	290
76	Combinaison de miroirs local et distant (récupération après sinistre intégrée à la sauvegarde : service haute disponibilité - HP UX uniquement) .....	292
77	Sauvegarde de snapshot .....	297
78	Baie de disques simple - hôte double (sauvegarde avec performance optimale et temps d'indisponibilité nul) .....	302
79	Baies de disques multiples - hôte double .....	303
80	Hôtes d'application multiples - hôte de sauvegarde simple .....	304
81	Baie(s) de disques - hôte simple .....	305
82	Acteurs du modèle de sauvegarde traditionnel .....	310
83	Acteurs du modèle de sauvegarde VSS .....	310
84	Topologie de sauvegarde actuelle de XYZ .....	321
85	Topologie de sauvegarde proposée pour XYZ .....	326
86	Paramètres d'entrée .....	327
87	Résultats .....	327
88	Topologie de sauvegarde actuelle d'ABC Le Cap .....	336
89	Environnement d'entreprise d'ABC .....	340
90	Environnement de sauvegarde d'entreprise d'ABC Le Cap .....	343
91	Paramètres d'entrée .....	345
92	Résultats .....	345
93	Génération de sauvegarde .....	356
94	Sauvegarde Incr1 et copie automatisée de supports .....	360
95	Sauvegarde complète et copie automatisée de supports .....	362
96	Présentation des sessions de sauvegarde et de copie automatisée des supports .....	363
97	Sauvegarde complète de base de données et copie automatisée de supports .....	364
98	Présentation des sessions de sauvegarde et de copie automatisée des supports .....	365



---

# Tableaux

1 Informations sur cette édition .....	19
2 Conventions typographiques .....	29
3 Comportement relatif à la sauvegarde .....	91
4 Comportement relatif à la sauvegarde .....	93
5 Comportement relatif à la sauvegarde .....	96
6 Comparaison entre la sauvegarde complète et la sauvegarde incrémentale .....	98
7 Références relatives des différentes sauvegardes .....	102
8 Planification échelonnée .....	116
9 Méthodes de duplication de données Data Protector .....	122
10 Agent de support Data Protector requis pour le contrôle des lecteurs ....	185
11 Agent de support Data Protector requis pour le contrôle des robots .....	185
12 Groupes d'utilisateurs prédéfinis Data Protector .....	203
13 Fonctionnalité ARM .....	230
14 Avantages de l'utilisation de VSS .....	311
15 Environnement matériel et logiciel de XYZ .....	320
16 Environnement proposé .....	324
17 Planification répartie .....	329
18 Sauvegardes complètes à distance vers la bibliothèque HP DLT 4115 .....	330
19 Taille de l'environnement de sauvegarde .....	335
20 Temps d'indisponibilité maximum pour la récupération .....	338
21 Durée de conservation nécessaire des données .....	338
22 Quantité de données à sauvegarder .....	339

23	Quantité de données à sauvegarder dans cinq ans .....	339
24	Configuration des cellules d'ABC .....	342
25	Utilisation des pools de supports d'ABC .....	349
26	Planification répartie pour ABC Le Cap .....	350
27	Configuration de spécification de sauvegarde pour ABC .....	351

---

# 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
B6960-96001	Août 2006	Data Protector Version A.06.00
B6960-96035	Novembre 2008	Data Protector Version A.06.10
B6960-90151	Septembre 2009	Data Protector Version A.06.11
	Mars 2011	Data Protector Version A.06.20



---

# A propos de ce manuel

Ce manuel décrit les concepts de Data Protector. La lecture de ce manuel donne une bonne compréhension des concepts fondamentaux et du modèle sur lequel est construit Data Protector.

## Public visé

Ce manuel s'adresse aux utilisateurs qui s'intéressent aux concepts de fonctionnement de Data Protector et aux personnes responsables de la planification de stratégies de sauvegarde pour leur entreprise. Selon le niveau de précision requis, vous pouvez également utiliser ce manuel conjointement à l'aide en ligne 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 Data Protector sont disponibles au format PDF. Vous pouvez installer les fichiers PDF lors de l'installation de Data Protector en sélectionnant le composant *Documentation en français (guides, aide)* sous Windows ou le composant *OB2-DOCS* sous UNIX. Les guides sont alors placés dans le répertoire `répertoire_Data_Protector\docs` sous Windows ou `/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*, cliquez sur **Storage Software**, 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 de ce produit. Il est conçu pour être utilisé avec l'aide en ligne qui se concentre sur les tâches du logiciel.

- *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 après sinistre HP Data Protector*

Ce guide explique comment planifier, préparer, tester et exécuter une récupération après sinistre.

- *Guide d'intégration HP Data Protector*

Les guides d'intégration expliquent comment configurer et utiliser Data Protector pour sauvegarder et restaurer différentes bases de données et applications. Ils s'adressent aux opérateurs ou aux administrateurs de sauvegarde. Il existe six guides :

- *Guide d'intégration HP Data Protector pour les applications Microsoft : SQL Server, SharePoint Portal Server et Exchange Server*

Ce guide décrit l'intégration de Data Protector avec les applications Microsoft suivantes : Microsoft SQL Server, Microsoft SharePoint Server et Microsoft Exchange Server.

- *Guide d'intégration HP Data Protector pour Oracle et SAP*

Ce guide décrit l'intégration de Data Protector avec Oracle Server, SAP R/3 et SAP 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 UDB et Lotus Notes/Domino Server.

- *Guide d'intégration HP Data Protector pour Sybase, Network Node Manager et le serveur NDMP (Network Data Management Protocol)*

Ce guide décrit l'intégration de Data Protector avec Sybase Server, HP Network Node Manager et le serveur NDMP (Network Data Management Protocol).

- *Guide d'intégration HP Data Protector pour les environnements de virtualisation*

Ce guide décrit l'intégration de Data Protector avec les environnements de virtualisation suivants : infrastructure virtuelle VMware et VMware vSphere, Microsoft Hyper-V et Citrix XEN Server.

- *Guide d'intégration HP Data Protector pour Microsoft Volume Shadow Copy Service*

Ce guide décrit l'intégration de Data Protector avec Microsoft Volume Shadow Copy Service. Il donne également des précisions sur le module d'écriture de l'application.

- *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 sous Windows.

- *Guide conceptuel ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*

Ce guide décrit les concepts 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*, lequel met l'accent sur les tâches du logiciel, et avec 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 P6000 EVA Disk Array Family, HP StorageWorks P9000 XP Disk Array Family, HP StorageWorks P4000 SAN Solutions, EMC Symmetrix Remote Data Facility et TimeFinder. Il s'adresse aux opérateurs ou aux administrateurs de sauvegarde. Il décrit la sauvegarde avec temps d'indisponibilité nul, la restauration instantanée, ainsi que 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 comment configurer et utiliser Data Protector pour effectuer des sauvegardes avec temps d'indisponibilité nul, des restaurations instantanées ainsi que des restaurations standard de bases de données Oracle Server, SAP R/3, Microsoft Exchange Server et Microsoft SQL Server.

- *Guide d'utilisation de l'extension de restauration granulaire HP Data Protector pour Microsoft SharePoint Server*

Ce guide décrit comment configurer et utiliser l'extension de restauration granulaire Data Protector pour Microsoft SharePoint Server. L'extension de restauration granulaire Data Protector est intégrée à l'application Administration centrale de Microsoft SharePoint Server et vous permet de récupérer des éléments individuels. Ce guide s'adresse aux administrateurs de Microsoft SharePoint Server et aux administrateurs de sauvegarde Data Protector.

- *Guide d'utilisation de l'extension de restauration granulaire HP Data Protector pour VMware vSphere*

Ce guide décrit comment configurer et utiliser l'extension de restauration granulaire Data Protector pour VMware vSphere. L'extension de restauration granulaire Data Protector est intégrée à VMware vCenter Server et vous permet de récupérer des éléments individuels. Ce guide s'adresse aux utilisateurs de VMware vCenter Server et aux administrateurs de sauvegarde Data Protector.

- *Guide de l'utilisateur HP Data Protector Media Operations*

Ce guide contient des informations sur le suivi et la gestion des supports de stockage hors ligne à l'intention des administrateurs réseau chargés de la maintenance et de la sauvegarde des systèmes. 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 6.20. Il donne également des informations sur les conditions requises pour l'installation, les correctifs requis et les limitations, ainsi que sur les problèmes connus et leurs solutions.

- *Références, notes de publication et annonces produits HP Data Protector pour les intégrations avec HP Operations Manager*

Ce guide remplit une fonction similaire pour l'intégration HP Operations Manager.

- *Références, notes de publication et annonces produits HP Data Protector Media Operations*

Ce guide remplit une fonction similaire pour Media Operations.

- *Guide de référence de l'interface de ligne de commande HP Data Protector*



Ce guide décrit l'interface de ligne de commande de Data Protector, les options et la syntaxe des commandes, et fournit quelques exemples de commandes simples.

## Aide en ligne

Data Protector comporte des rubriques d'aide et une aide contextuelle (F1) 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-ROM d'installation sans installer 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 en cliquant sur `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	Guide de référence de l'interface de ligne de commande
Concepts	Guide conceptuel
DR	Guide de récupération après sinistre
GS	Guide de démarrage rapide
GRE-SPS	Guide d'utilisation de l'extension de restauration granulaire pour Microsoft SharePoint Server
GRE-VMware	Guide d'utilisation de l'extension de restauration granulaire pour VMware vSphere
Aide	Aide en ligne

<b>Abréviation</b>	<b>Guide</b>
IG-IBM	Guide d'intégration pour les applications IBM : Informix, DB2 et Lotus Notes/Domino
IG-MS	Guide d'intégration pour les applications Microsoft : SQL Server, SharePoint Server et Exchange Server
IG-O/S	Guide d'intégration pour Oracle et SAP
IG-OMU	Guide d'intégration pour HP Operations Manager sous UNIX
IG-OMW	Guide d'intégration pour HP Operations Manager sous Windows
IG-Var	Guide d'intégration pour Sybase, Network Node Manager et le serveur NDMP (Network Data Management Protocol)
IG-VirtEnv	Guide d'intégration pour les environnements de virtualisation : VMware, Microsoft Hyper-V et Citrix XEN Server
IG-VSS	Guide d'intégration pour Microsoft Volume Shadow Copy Service
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
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

## Organisation

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

	Aide	GS	Concepts	Install.	Dépan.	DIR	PA	Guides intégration							ZDB		MO		CLI	
	GS	Install.	Dépan.	DIR	PA	MS	O/S	IBM	Var	OV	OVU	OVOW	Concept	Admin	IG	GS	Utilisat.	PA		MPE/IX
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
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		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		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 les intégrations avec les applications logicielles suivantes :

Application logicielle	Guides
HP Network Node Manager (NNM)	IG-Var
HP Operations Manager	IG-OMU, IG-OMW
IBM DB2 UDB	IG-IBM
Informix Server	IG-IBM
Lotus Notes/Domino Server	IG-IBM
Media Operations	Utilisateur MO
Microsoft Exchange Server	IG-MS, ZDB IG

<b>Application logicielle</b>	<b>Guides</b>
Microsoft Hyper-V	IG-VirtEnv
Microsoft SharePoint Server	IG-MS, ZDB IG, GRE-SPS
Microsoft SQL Server	IG-MS, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-VSS
Serveur NDMP (Network Data Management Protocol)	IG-Var
Oracle Server	IG-O/S, ZDB IG
SAP MaxDB	IG-O/S
SAP R/3	IG-O/S, ZDB IG
Sybase Server	IG-Var
VMware vSphere	IG-VirtEnv, GRE-VMware

Le tableau ci-dessous vous permet de repérer le guide à consulter pour obtenir des détails sur les intégrations avec les familles de baies de disques suivantes :

<b>Famille de baies de disques</b>	<b>Guides</b>
EMC Symmetrix	Tous les guides ZDB
HP StorageWorks P4000 SAN Solutions	Guide conceptuel ZDB, Guide de l'administrateur ZDB, IG-VSS
HP StorageWorks P6000 EVA Disk Array Family	Tous les guides ZDB
HP StorageWorks P9000 XP Disk Array Family	Tous les guides ZDB

# Conventions typographiques et symboles

Tableau 2 Conventions typographiques

Convention	Élément
Texte bleu : <a href="#">Tableau 2</a> à la page 29	Renvois et adresses électroniques
Texte souligné en bleu : <a href="http://www.hp.com">http://www.hp.com</a>	Adresses de sites Web
Texte <i>italique</i>	Texte mis en évidence
Texte non proportionnel	<ul style="list-style-type: none"><li>• Noms des fichiers et des répertoires</li><li>• Sortie du système</li><li>• Code</li><li>• Commandes et leurs arguments, valeurs des arguments</li></ul>
Texte <i>non proportionnel, italique</i>	<ul style="list-style-type: none"><li>• Variables de code</li><li>• Variables de commande</li></ul>
Texte non proportionnel, gras	Texte à espacement fixe 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 :**

Fournit des explications ou des instructions spécifiques.

---

---

📝 **REMARQUE :**

Fournit des informations complémentaires.

---

💡 **CONSEIL :**

Propose des conseils utiles et des raccourcis.

## 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.

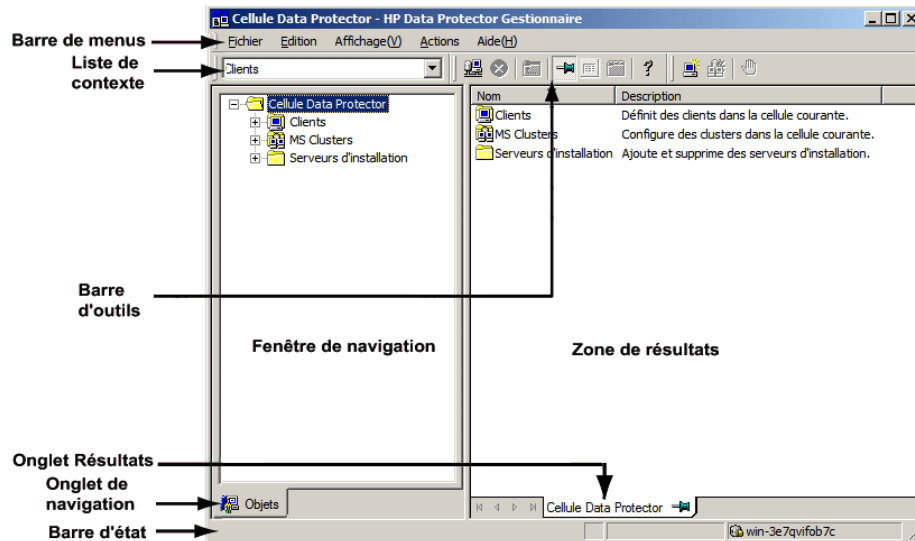


Figure 1 Interface utilisateur graphique de Data Protector

## Informations générales

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

## Assistance technique HP

Pour des 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 ou des produits
- Numéro d'enregistrement d'assistance technique (si vous en avez un)
- Numéro de série du produit
- Messages d'erreur
- Type et niveau de révision du système d'exploitation
- Vos questions, aussi détaillées que possible

## Service d'enregistrement

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://h20230.www2.hp.com/selfsolve/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](mailto:DP.DocFeedback@hp.com). Toutes les soumissions deviennent propriété de HP.



---

# 1 A propos de la sauvegarde et de Data Protector

## Dans ce chapitre

Ce chapitre propose un tour d'horizon des concepts de sauvegarde et de restauration. Vous y trouverez une présentation de l'architecture de Data Protector, de la gestion de supports, des interfaces utilisateur, des périphériques de sauvegarde et d'autres caractéristiques. Le chapitre se conclut par une présentation de la configuration de Data Protector et d'autres tâches requises pour l'installation de Data Protector.

Il s'organise comme suit :

“A propos de Data Protector” à la page 33

“Présentation des sauvegardes et des restaurations” à la page 37

“Architecture de Data Protector” à la page 39

“Environnements d'entreprise” à la page 44

“Gestion des supports” à la page 48

“Périphériques de sauvegarde” à la page 49

“Interfaces utilisateur” à la page 50

“Présentation des tâches nécessaires à la configuration de Data Protector” à la page 55

## A propos de Data Protector

HP Data Protector est une solution de sauvegarde qui offre une protection fiable des données et une grande facilité d'accès aux données de votre entreprise. Data Protector propose une fonctionnalité complète de sauvegarde et de restauration spécialement conçue pour les environnements à l'échelle de l'entreprise et les environnements distribués. La liste suivante décrit les principales caractéristiques de Data Protector :

- **Architecture évolutive et d'une grande flexibilité**

Data Protector peut être utilisé dans des environnements allant d'un simple système à des milliers de systèmes disséminés sur plusieurs sites. Grâce au concept de composant réseau de Data Protector, des éléments de l'infrastructure de sauvegarde peuvent être intégrés dans la topologie en fonction des besoins de l'utilisateur. Les nombreuses options de sauvegarde et possibilités offertes pour configurer l'infrastructure de sauvegarde vous permettent de mettre en œuvre pratiquement toutes les configurations de votre choix. Data Protector permet en outre d'utiliser des concepts de sauvegarde avancés tels que la sauvegarde synthétique et la sauvegarde de disque en plusieurs étapes.

- **Administration facile et centralisée**

Grâce à son interface graphique simple à utiliser, Data Protector vous permet d'administrer la totalité de votre environnement de sauvegarde à partir d'un seul système. Pour en faciliter l'exploitation, l'interface graphique peut être installée sur divers systèmes pour permettre à plusieurs administrateurs d'accéder à Data Protector via leurs terminaux installés en local. Il est même possible de gérer plusieurs environnements de sauvegarde à partir d'un seul système. Son interface de ligne de commande vous permet de gérer Data Protector à l'aide de scripts.

- **Fonction de sauvegarde haute performance**

Data Protector vous permet d'effectuer des sauvegardes sur plusieurs centaines de périphériques de sauvegarde simultanément. Il prend en charge les périphériques haut de gamme dans les très grandes bibliothèques. Vous pouvez choisir parmi un grand nombre de types de sauvegarde afin d'utiliser celui qui répondra le mieux à vos besoins : sauvegarde en local, en réseau, en ligne, sauvegarde d'image disque, sauvegarde synthétique, sauvegarde avec mise en miroir d'objets et prise en charge intégrée de flux de données parallèles.

- **Sécurité des données**

Pour améliorer la sécurité de vos données, Data Protector vous permet de crypter vos sauvegardes afin de les protéger vis à vis des autres. Deux techniques de cryptage des données sont disponibles dans Data Protector : le cryptage sur logiciel et le cryptage sur lecteur.

- **Prise en charge des environnements mixtes**

Data Protector prenant en charge des environnements hétérogènes, la plupart des caractéristiques sont communes aux plates-formes UNIX et Windows. Le Gestionnaire de cellule UNIX et Windows peut contrôler toutes les plates-formes client prises en charge (UNIX, Windows et Novell NetWare). L'interface utilisateur de Data Protector permet l'accès à l'ensemble de ses fonctionnalités sur toutes les plates-formes.

- **Installation facile pour les environnements mixtes**

Le concept de Serveur d'installation simplifie l'installation et les procédures de mise à niveau. Pour installer à distance des clients UNIX, vous devez disposer d'un Serveur d'installation pour UNIX. Pour installer à distance des clients Windows, vous devez disposer d'un Serveur d'installation pour Windows. L'installation à distance peut être réalisée à partir de n'importe quel client sur lequel est installée l'interface graphique de Data Protector. Pour connaître les plates-formes prises en charge par le Serveur d'installation, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

- **Haute disponibilité des données**

Vos activités commerciales doivent pouvoir se poursuivre 24 heures sur 24. Data Protector vous permet de répondre à cette exigence. Dans l'environnement professionnel d'aujourd'hui, partagé à l'échelle mondiale, les ressources d'informations d'une entreprise ainsi que les applications dédiées aux services client doivent être disponibles à tout moment. Data Protector vous permet de satisfaire à ces exigences de disponibilité grâce aux avantages suivants :

- Intégration avec les clusters pour garantir un fonctionnement sécurisé et la possibilité de sauvegarder des nœuds virtuels. Pour obtenir une liste des clusters pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Activation du Gestionnaire de cellule Data Protector lui-même pour une exécution sur un cluster.
- Prise en charge des API (interfaces de programmation d'application) de base de données en ligne les plus courantes.
- Intégration à des solutions avancées de haute disponibilité telles que EMC Symmetrix, HP StorageWorks P6000 EVA Disk Array Family, HP StorageWorks P9000 XP Disk Array Family ou HP StorageWorks P4000 SAN Solutions.
- Mise à disposition de diverses méthodes de récupération après sinistre pour les plates-formes Windows et UNIX.
- Mise à disposition de méthodes de duplication des données sauvegardées pendant et après la sauvegarde en vue d'améliorer la tolérance aux pannes ou à des fins de redondance.

- **Opérations liées aux objets sauvegarde**

Différentes techniques avancées permettent d'effectuer des opérations sur des objets sauvegarde individuels, offrant ainsi la possibilité de choisir la stratégie de sauvegarde et d'archivage appropriée. Il s'agit notamment de la copie d'objets d'un support vers un autre, utile en cas de sauvegarde de disque en plusieurs étapes et d'archivage, et de la consolidation, à partir de sauvegardes incrémentales, de plusieurs versions d'un objet en une sauvegarde complète unique. Pour compléter cette fonctionnalité, il est également possible de vérifier à la fois les objets originaux et les objets copiés ou consolidés.

- **Procédure de restauration facile**

Data Protector comprend une base de données qui effectue un suivi des données : par exemple, pour chaque fichier, le système dont il provient et le support précis sur lequel il est stocké. Pour restaurer n'importe quelle partie d'un système, il vous suffit d'explorer les fichiers et les répertoires. Ceci permet à l'utilisateur d'accéder rapidement et facilement aux données à restaurer.

- **Opération automatisée ou sans surveillance**

Grâce à sa base de données interne, Data Protector conserve des informations sur chacun des supports Data Protector et sur les données qu'ils hébergent. Data Protector propose une fonctionnalité de pointe en matière de gestion des supports. Par exemple, il enregistre la période pendant laquelle une sauvegarde donnée doit rester disponible pour la restauration, ainsi que les supports qui peuvent être (ré)utilisés pour les sauvegardes.

Cette fonctionnalité est complétée par le support de très grandes bibliothèques, ce qui permet une opération sans surveillance sur plusieurs jours ou semaines (rotation automatique des supports). De plus, lorsque vous connectez de nouveaux disques aux systèmes, Data Protector est en mesure de les détecter automatiquement (ou de les reconnaître) et de les sauvegarder. Il est donc inutile d'adapter les configurations manuellement.

- **Gestion des services**

Data Protector est la première solution de gestion de sauvegarde et de restauration à prendre en charge la gestion des services. L'intégration aux solutions de gestion du temps de réponse des applications (ARM) et d'intégration des sources de données (DSI) contribue efficacement à la gestion du niveau de service (SLM) et au respect des accords sur le niveau de service (SLA) en fournissant des données pertinentes aux systèmes de gestion et de planification.

L'intégration DSI fournit une série de scripts et de fichiers de configuration permettant aux utilisateurs d'ajouter leurs propres requêtes à l'aide des fonctions de génération de rapports de Data Protector.

- **Fonctionnalité Contrôle, rapports et notifications**

Les fonctions Web avancées pour la génération de rapports et la notification vous permettent d'afficher l'état des sauvegardes, de contrôler les opérations de sauvegarde en cours et de personnaliser les rapports en toute simplicité. Les rapports peuvent être générés au moyen de l'interface Data Protector ou à l'aide de la commande `omnirpt` sur les systèmes fonctionnant sous UNIX ou Windows, ainsi que par le biais de rapports Web générés en ligne avec Java.

Vous pouvez programmer la génération de rapports à un moment déterminé ou en fonction d'une série d'événements prédéfinis, par exemple à la fin d'une session de sauvegarde ou lorsqu'une requête de montage est émise.

Par ailleurs, la fonctionnalité d'audit de Data Protector vous permet de collecter un sous-ensemble d'informations sur la session de sauvegarde et fournit une synthèse des opérations de sauvegarde. Les informations sur la session de sauvegarde sont enregistrées dans les fichiers journaux d'audit.

- **Intégration aux applications en ligne**

Data Protector permet de sauvegarder en ligne des objets de bases de données Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint Server, Oracle, Informix Server, SAP R/3, SAP MaxDB, Lotus Notes/Domino Server, IBM DB2 UDB et Sybase, ainsi que des objets VMware Virtual Infrastructure et Hyper-V. Pour obtenir la liste des versions prises en charge pour un système d'exploitation particulier, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

- **Intégration à d'autres produits**

En outre, Data Protector s'intègre à EMC Symmetrix, Microsoft Cluster Server, MC/ServiceGuard et d'autres produits.

Pour obtenir une documentation détaillée décrivant les fonctions de Data Protector, y compris les intégrations, ainsi que les informations les plus récentes en termes de prise en charge des intégrations et des plates-formes, reportez-vous à la page d'accueil de HP Data Protector à l'adresse <http://www.hp.com/support/manuals>.

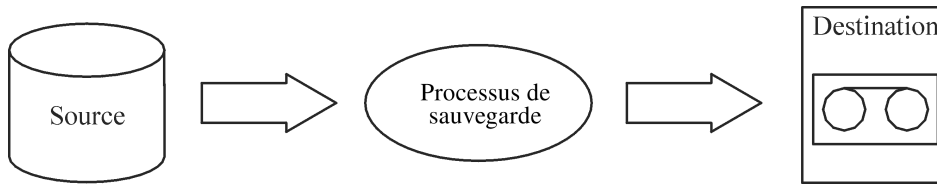
## Présentation des sauvegardes et des restaurations

Vous trouverez dans cette section les principes de base relatifs aux concepts de sauvegarde et de restauration.

### Qu'est-ce qu'une sauvegarde ?

Une sauvegarde est une opération consistant à créer une copie des données sur un support de stockage. Cette copie est stockée et conservée pour une utilisation ultérieure, au cas où l'original serait détruit ou endommagé.

Pour obtenir une présentation globale d'une sauvegarde, reportez-vous à la [Figure 2](#) à la page 38 ci-dessous.



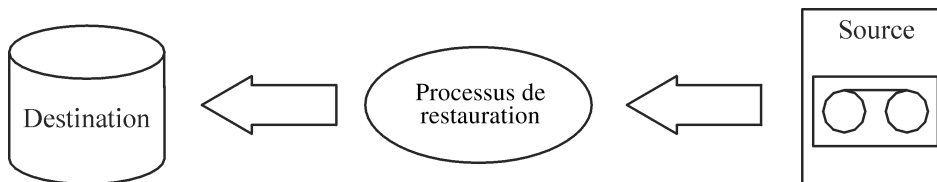
**Figure 2 Processus de sauvegarde**

Dans la plupart des cas, la **source** correspond à des données enregistrées sur un disque, par exemple des fichiers, des répertoires, des bases de données et des applications. Si la sauvegarde est réalisée dans l'optique d'une récupération après sinistre, il faut qu'elle soit cohérente.

Le logiciel qui copie les données vers la destination est appelé "application de sauvegarde". La **destination** est un périphérique de sauvegarde, tel qu'un lecteur de bande (y compris le support sur lequel les données sont écrites).

## Qu'est-ce qu'une restauration ?

Une restauration est une opération consistant à recréer des données originales à partir d'une copie de sauvegarde. Ce concept regroupe la préparation et la restauration proprement dite des données, ainsi que certaines actions après restauration qui permettent de rendre les données exploitables.

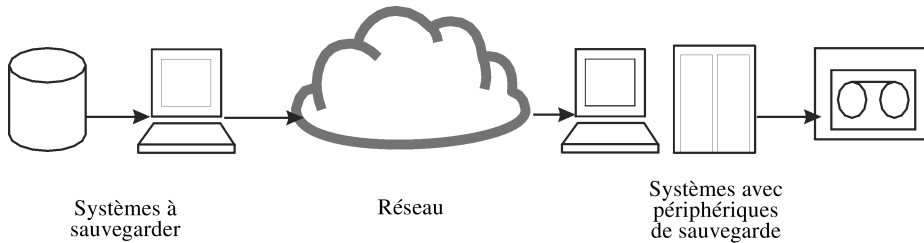


**Figure 3 Processus de restauration**

La **source** est une copie de sauvegarde. Une application de restauration est un logiciel qui écrit les données dans un emplacement de destination. La **destination** est généralement un disque sur lequel les données d'origine sont écrites.

## Sauvegarde d'un environnement réseau

Lorsque des sauvegardes sont effectuées dans un environnement réseau, les données sont transférées via le réseau à partir des systèmes à sauvegarder vers des supports, sur des systèmes dotés de périphériques de sauvegarde, sur lesquels les données sont stockées.



**Figure 4 Sauvegarde réseau**

Pour réaliser la sauvegarde d'un environnement réseau, vous avez besoin d'une application qui vous permette de :

- raccorder des périphériques de sauvegarde à n'importe quel système du réseau  
Cela permet d'effectuer des sauvegardes locales de systèmes présentant de gros volumes de données et des sauvegardes réseau en vue de réduire les coûts liés aux périphériques de sauvegarde.
- diriger le flux des données de sauvegarde vers n'importe quel chemin réseau
- diriger les données de sauvegarde hors du réseau LAN et vers un réseau SAN lorsque le volume des données ou l'encombrement du réseau rendent inefficace le transfert de données via le réseau LAN
- gérer les opérations de sauvegarde à partir de n'importe quel système
- réaliser l'intégration dans la structure de l'administration informatique
- prendre en charge la sauvegarde de nombreux types de systèmes différents

## Architecture de Data Protector

La cellule Data Protector, représentée à la [Figure 5](#) à la page 40, est un environnement réseau doté d'un **Gestionnaire de cellule**, de **systèmes client** et de **périphériques**. Le Gestionnaire de cellule constitue le point de contrôle central sur lequel le logiciel Data Protector est installé. Après avoir installé le logiciel Data Protector, vous pouvez ajouter des systèmes à sauvegarder. Ces derniers deviennent des systèmes client de Data Protector, qui font partie de la cellule. Lorsque Data Protector sauvegarde des fichiers, il les enregistre sur des supports situés dans les périphériques de sauvegarde.

La **base de données interne (IDB) de Data Protector** assure un suivi des fichiers que vous sauvegardez, de sorte qu'il vous suffit de l'explorer pour récupérer facilement la totalité du système ou seulement certains fichiers.

Data Protector simplifie les tâches de sauvegarde et de restauration. Vous pouvez effectuer une sauvegarde instantanée (ou interactive) au moyen de l'interface utilisateur

de Data Protector. Vous pouvez également planifier vos sauvegardes pour qu'elles s'exécutent sans surveillance.

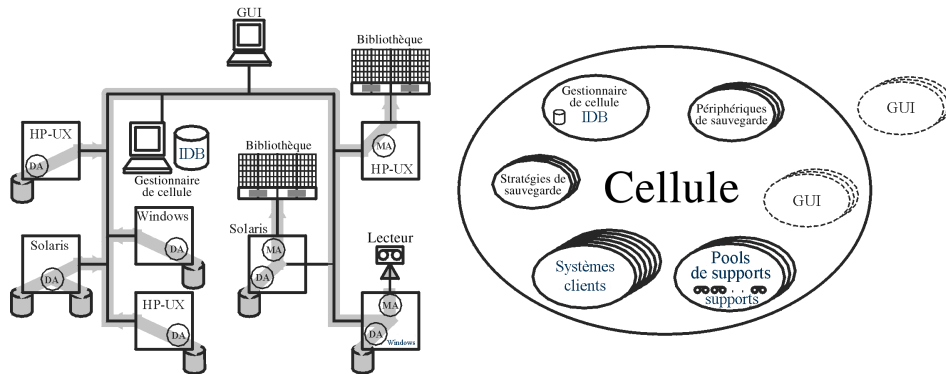


Figure 5 Cellule Data Protector (description physique et logique)



#### REMARQUE :

L'interface utilisateur et les systèmes Gestionnaire de cellule peuvent s'exécuter sur des systèmes d'exploitation UNIX et Windows ; il n'est toutefois pas nécessaire qu'ils s'exécutent sur le même système d'exploitation. Pour obtenir la liste des systèmes d'exploitation pris en charge pour un composant Data Protector particulier, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

### Gestionnaire de cellule

Le Gestionnaire de cellule est le système le plus important de la cellule. Le Gestionnaire de cellule :

- gère la cellule à partir d'un point central
- contient la base de données IDB  
La base de données IDB contient des informations relatives aux sauvegardes, telles que les durées des sauvegardes et les ID des supports et des sessions.
- exécute le logiciel Data Protector de base
- exécute les Gestionnaires de session qui démarrent et arrêtent les sessions de sauvegarde et de restauration, et enregistrent des informations relatives aux sessions dans la base de données IDB.



## Systemes à sauvegarder

Les systemes client que vous souhaitez sauvegarder doivent disposer d'un Agent de disque (DA), également appelé **Agent de sauvegarde**, installé. Pour pouvoir sauvegarder les integrations de bases de donnees en ligne, vous devez installer l'**Agent d'application**. Dans le reste du guide, le terme "Agent de disque" est utilise pour designer les deux agents. L'Agent de disque lit ou ecrit des donnees a partir d'un disque sur le systeme et envoie ou recoit des donnees d'un Agent de support. L'Agent de disque est également installé sur le Gestionnaire de cellule, ce qui vous permet de sauvegarder des donnees sur le Gestionnaire de cellule, la configuration de Data Protector et la base de donnees IDB.

## Systemes dotés de peripheriques de sauvegarde

Les systemes client auxquels sont connectés les peripheriques de sauvegarde doivent disposer d'un **Agent de support** (MA) Data Protector installé. Ces systemes client sont également appelés **serveurs de lecteurs**. Un peripherique de sauvegarde peut être connecté à n'importe quel systeme et pas uniquement au Gestionnaire de cellule. Un Agent de support lit ou ecrit des donnees depuis ou vers un support du peripherique et envoie ou recoit des donnees de l'Agent de disque.

## Systemes dotés d'une interface utilisateur

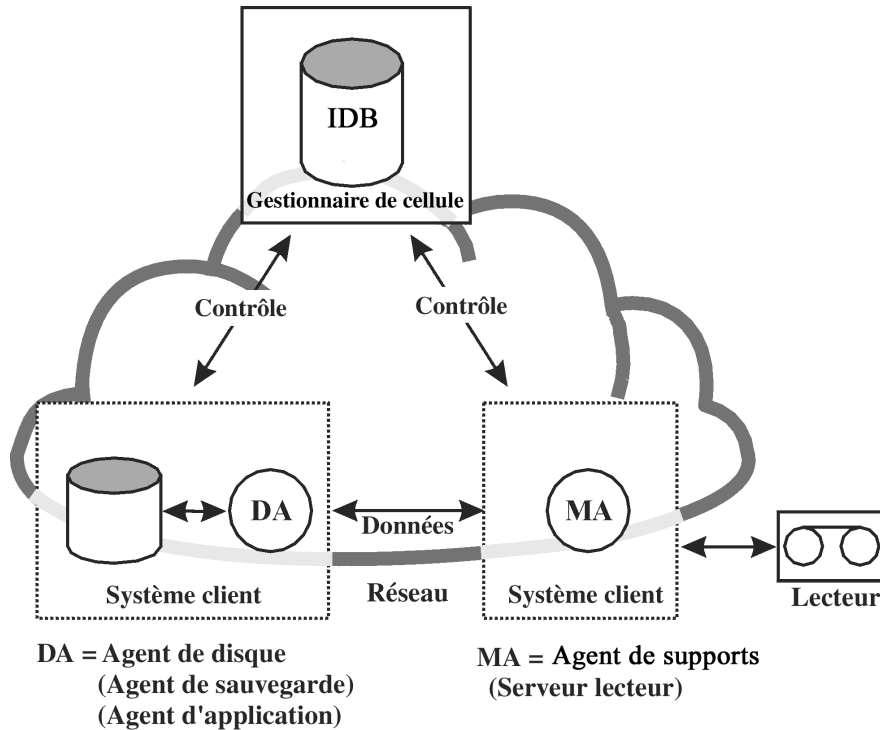
Vous pouvez gérer Data Protector à partir de n'importe quel systeme sur le reseau sur lequel l'interface utilisateur graphique Data Protector est installée. Le Gestionnaire de cellule peut donc être installé dans une salle informatique, tandis que vous gérez Data Protector à partir de votre ordinateur de bureau.

## Serveur d'installation

Le **Serveur d'installation** contient un référentiel des ensembles de logiciels Data Protector pour une architecture spécifique. Par défaut, le Gestionnaire de cellule est également un Serveur d'installation. Les environnements mixtes requièrent au moins deux serveurs d'installation : l'un pour les systemes UNIX et l'autre pour les systemes Windows.

## Operatiions effectuées dans la cellule

Le Gestionnaire de cellule Data Protector contrôle les sessions de sauvegarde et de restauration, qui effectuent respectivement toutes les actions requises pour une sauvegarde ou une restauration (voir [Figure 6](#) à la page 42).



**Figure 6 Opération de sauvegarde ou de restauration**

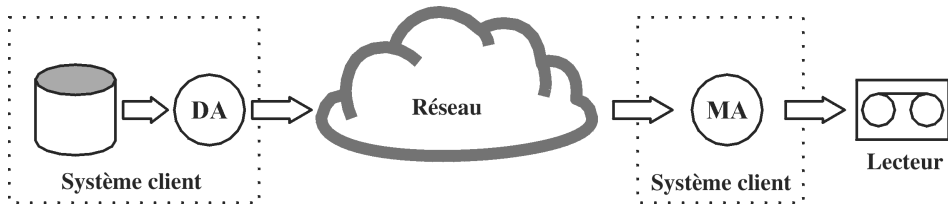
## Sessions de sauvegarde

### Qu'est-ce qu'une session de sauvegarde ?

Une session de sauvegarde (voir [Figure 7](#) à la page 43) est une procédure consistant à créer une copie de données sur un support de stockage. Son démarrage peut se faire de deux manières différentes : interactivement par un opérateur ou sans surveillance à l'aide du Planificateur de Data Protector.

### Fonctionnement

Le Gestionnaire de session de sauvegarde démarre les Agents de support et les Agents de disque, contrôle la session et stocke les messages générés dans la base de données IDB. Les données sont lues par l'Agent de disque et envoyées à un Agent de support, qui les enregistre sur les supports.



**Figure 7 Session de sauvegarde**

Les sessions de sauvegarde sont généralement plus complexes que celle montrée à la [Figure 7](#) à la page 43. Plusieurs Agents de disque lisent les données de plusieurs disques en parallèle et les envoient à un ou plusieurs Agents de support. Pour obtenir des informations complémentaires sur les sessions de sauvegarde complexes, reportez-vous au [Chapitre 7](#) à la page 237.

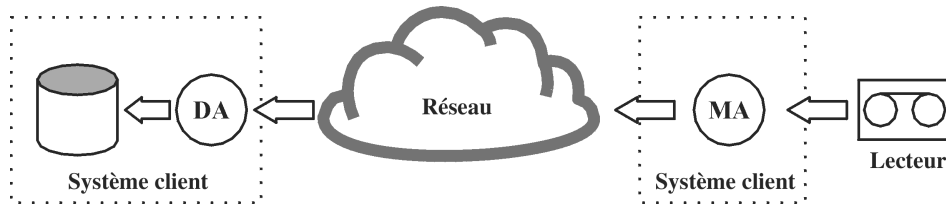
## Sessions de restauration

### Qu'est-ce qu'une session de restauration ?

Une session de restauration (voir [Figure 8](#) à la page 44) est une procédure consistant à restaurer vers un disque des données préalablement sauvegardées. La session de restauration peut être lancée de façon interactive par un opérateur via l'interface utilisateur Data Protector.

### Fonctionnement

Une fois que vous avez sélectionné les fichiers à restaurer à partir d'une précédente sauvegarde, vous lancez le processus de restauration proprement dit. Le Gestionnaire de session de restauration démarre les Agents de support et les Agents de disque requis, contrôle la session et stocke les messages générés dans la base de données IDB. Les données sont lues par un Agent de support et envoyées à l'Agent de disque, qui les écrit sur des disques.



**Figure 8 Session de restauration**

Les sessions de restauration peuvent être plus complexes que celle montrée à la [Figure 8](#) à la page 44. Pour obtenir des informations complémentaires sur les sessions de restauration, reportez-vous au [Chapitre 7](#) à la page 237.

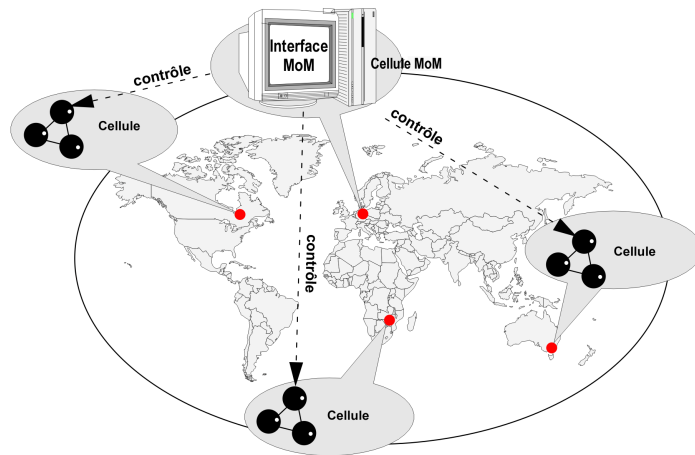
## Environnements d'entreprise

### Qu'est-ce qu'un environnement d'entreprise ?

Un environnement réseau d'entreprise (voir [Figure 9](#) à la page 45) est généralement composé d'un certain nombre de systèmes provenant de différents fournisseurs et dotés de différents systèmes d'exploitation. Les systèmes peuvent être installés dans des zones géographiques et des fuseaux horaires différents. Tous les systèmes sont connectés par des réseaux (LAN ou WAN) fonctionnant à divers débits.

### Quand utiliser un environnement d'entreprise ?

Cette solution peut être utilisée lorsque plusieurs sites séparés géographiquement requièrent l'application de **stratégies de sauvegarde** communes. Elle peut également être utilisée lorsque tous les départements d'un même site veulent partager les mêmes périphériques de sauvegarde.



**Figure 9 Environnement d'entreprise Data Protector étendu**

La configuration et la gestion des sauvegardes dans un environnement aussi hétérogène constituent des tâches complexes. Les fonctionnalités de Data Protector ont été conçues pour les simplifier au maximum. Pour obtenir des informations complémentaires sur le Manager-of-Managers (MoM), reportez-vous à la section [MoM](#) à la page 46.

## Séparation d'un environnement en plusieurs cellules

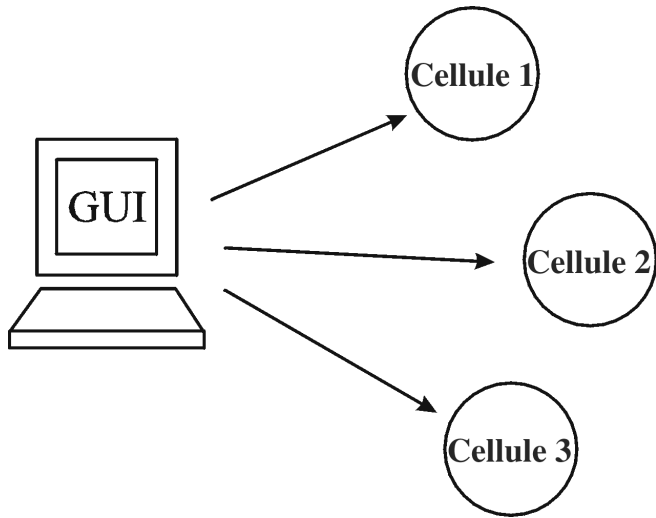
Vous souhaitez peut-être diviser les grands environnements en plusieurs cellules pour diverses raisons :

### Pourquoi séparer les grands environnements en plusieurs cellules ?

- Regroupement géographique des systèmes.
- Regroupement logique des systèmes, par exemple en services.
- Connexion réseau trop lente entre certains systèmes.
- Amélioration des performances.
- Contrôle administratif décentralisé.

Reportez-vous au [Chapitre 2](#) à la page 57, où vous trouverez une liste de points à prendre en considération au moment de la planification de votre environnement.

Data Protector vous permet de gérer plusieurs cellules à partir d'un même point.

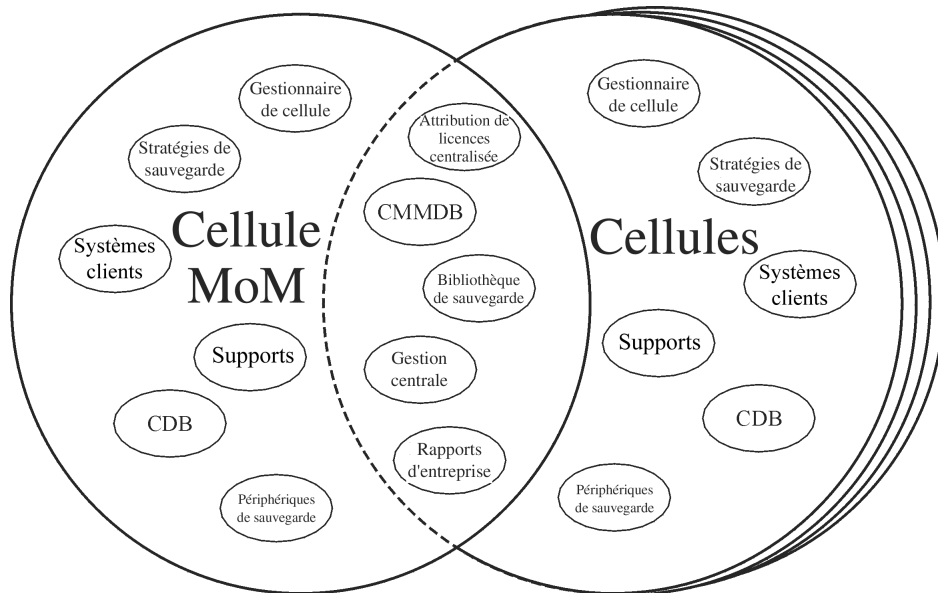


**Figure 10** Gestion centralisée de plusieurs cellules

## MoM

Le Manager-of-Managers de Data Protector permet de gérer les grands environnements avec plusieurs cellules. Vous pouvez ainsi regrouper plusieurs cellules au sein d'une unité plus grande appelée "environnement MoM", qui peut être gérée à partir d'un point central (voir [Figure 10](#) à la page 46). En outre, grâce au MoM, votre environnement de sauvegarde peut s'étendre de façon quasi illimitée. Vous pouvez ajouter de nouvelles cellules ou diviser des cellules existantes.

Un environnement MoM ne requiert pas de connexion réseau fiable entre les cellules Data Protector et la cellule centrale MoM, car seuls les contrôles sont envoyés via les connexions longue distance alors que les sauvegardes sont effectuées localement à l'intérieur de chaque cellule Data Protector. Cela présuppose en revanche que chaque cellule dispose de sa propre base de données de gestion des supports.



**Figure 11 Environnement Manager-of-Managers**

Le Manager-of-Managers présente les caractéristiques suivantes :

- **Référentiel de la gestion centralisée des licences**

Ce référentiel permet de simplifier la gestion des licences. Il est facultatif, mais particulièrement utile pour les environnements très vastes.

- **Base de données centralisée de gestion des supports (CMMDB)**

La CMMDB permet de partager des supports et périphériques entre plusieurs cellules d'un environnement MoM. Les périphériques d'une cellule donnée (qui utilise la CMMDB) sont ainsi accessibles aux autres cellules qui utilisent la CMMDB. Pour pouvoir être utilisée, la CMMDB doit résider dans la cellule MoM. Dans ce cas, il doit exister une connexion réseau fiable entre la cellule MoM et les autres cellules Data Protector. Notez que la centralisation de la base de données de gestion des supports n'est pas obligatoire.

- **Partage de bibliothèques**

Grâce à la CMMDB, vous pouvez partager des périphériques haut de gamme entre cellules dans l'environnement multicellules. Une cellule peut contrôler les systèmes robotiques desservant plusieurs périphériques connectés à des systèmes dans d'autres cellules. Même le chemin des données allant de l'Agent de disque à l'Agent de support peut traverser les "frontières" des cellules.

- **Rapports d'entreprise**

Le Manager-of-Managers Data Protector peut générer des rapports pour une seule cellule aussi bien que pour la totalité de l'environnement d'entreprise.

## Gestion des supports

Data Protector possède des fonctions de gestion de supports puissantes qui vous permettent de gérer simplement et efficacement un grand nombre de supports dans votre environnement, et ce de plusieurs façons :

### Fonctionnalité de gestion des supports

- Regroupement des supports en unités logiques appelées **pools de supports**, qui vous permettent de travailler sur de grands groupes de supports sans avoir à vous préoccuper de chacun en particulier.
- Suivi de tous les supports assuré par Data Protector qui garde en mémoire l'état de chacun d'eux, le délai d'expiration de la protection des données, la disponibilité des supports pour les sauvegardes et un catalogue des sauvegardes effectuées sur chaque support.
- Fonctionnement entièrement automatisé. Si Data Protector contrôle suffisamment de supports dans les périphériques de bibliothèque, la fonction de gestion des supports vous permet d'exécuter des sessions de sauvegarde sans intervention de l'opérateur.
- Rotation automatisée des supports, qui permet de les sélectionner pour les sauvegardes automatiques.
- Reconnaissance et prise en charge des codes-barres sur les périphériques de bibliothèque et périphériques silo importants disposant d'une prise en charge des codes-barres.
- Reconnaissance, suivi, affichage et gestion des supports utilisés par Data Protector dans les périphériques de bibliothèque et périphériques silo importants.
- Possibilité de centraliser les informations relatives aux supports et de les partager entre plusieurs cellules Data Protector.
- Création interactive ou automatisée de copies supplémentaires des données sur les supports.
- Prise en charge de la mise au coffre des supports.

### Qu'est-ce qu'un pool de supports ?

Data Protector utilise les pools de supports pour gérer ces derniers lorsqu'ils sont très nombreux. Un pool de supports est un regroupement logique de supports du **même** type physique et auxquels s'applique une politique d'utilisation commune (propriétés). L'utilisation est basée sur les données figurant sur le support. C'est vous qui décidez,

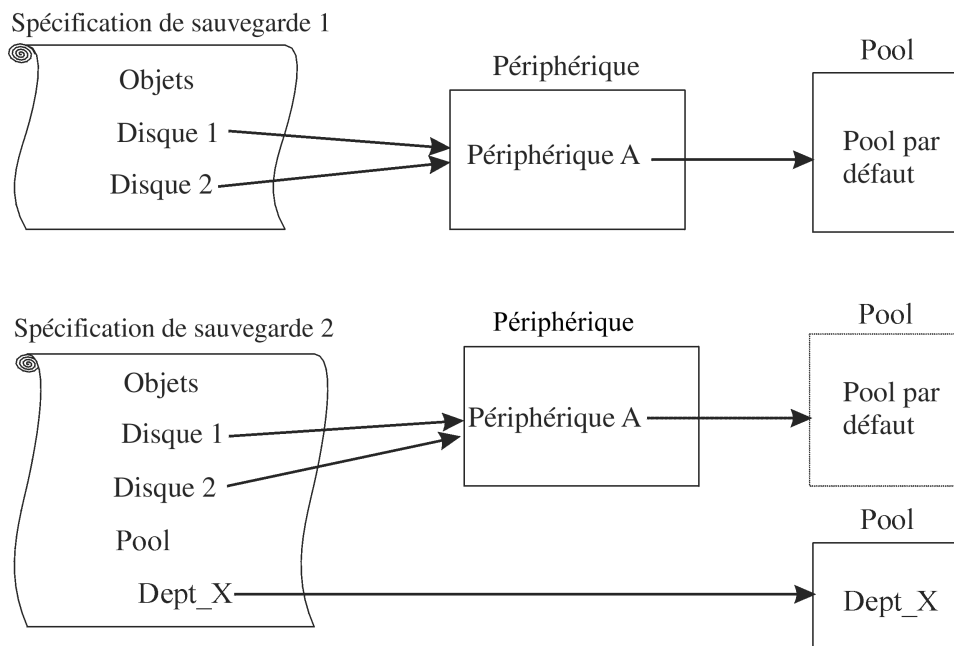


selon vos besoins, quelle doit être la structure des pools, leur nombre et, pour chacun des pools, le type de données figurant sur les supports qui en font partie.

Lorsque vous configurez un périphérique, un pool de supports par défaut est spécifié. Ce pool de supports est utilisé si aucun autre pool de supports n'est défini dans la spécification de sauvegarde.

## Périphériques de sauvegarde

Data Protector définit et modélise chaque périphérique comme un périphérique physique ayant des propriétés d'utilisation particulières (par exemple le pool par défaut). Ce concept de périphérique permet de configurer facilement et en souplesse les périphériques, et de les utiliser en accord avec les spécifications de sauvegarde. La définition des périphériques est stockée dans la base de données de gestion des supports Data Protector.



**Figure 12 Liens entre les spécifications de sauvegarde, les périphériques et les pools de supports**

La Figure 12 à la page 49 présente un schéma des relations entre les spécifications de sauvegarde, les périphériques et les pools de supports. Les périphériques sont désignés dans les spécifications de sauvegarde. Chaque périphérique est lié à un pool de supports. Ce pool de supports peut être modifié dans la spécification de

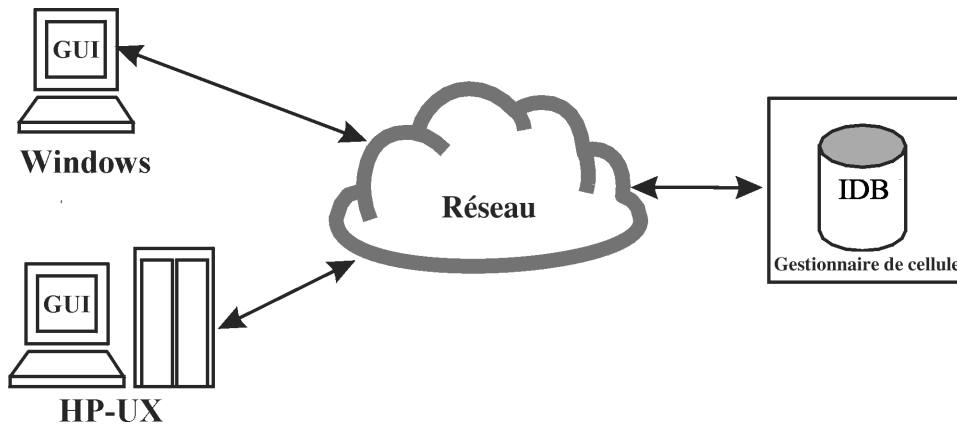
sauvegarde. Par exemple, la spécification de sauvegarde 2 fait appel au pool `Dept_X` au lieu du pool par défaut.

Data Protector prend en charge différents périphériques. Pour plus d'informations, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

## Interfaces utilisateur

Data Protector offre un accès facile à toutes les tâches de configuration et d'administration au moyen de l'interface utilisateur de Data Protector sur les plates-formes UNIX et Windows. Vous pouvez utiliser l'interface d'origine de Data Protector (sous Windows) ou l'interface Java de Data Protector (sous Windows et UNIX). Les deux interfaces peuvent fonctionner simultanément sur le même ordinateur. Une interface de ligne de commande est également disponible sur les plates-formes UNIX et Windows.

L'architecture de Data Protector vous offre la souplesse d'installation et d'utilisation de l'interface utilisateur de Data Protector. Il n'est pas nécessaire que l'interface utilisateur soit utilisée à partir du système Gestionnaire de cellule ; vous pouvez l'installer sur votre ordinateur de bureau. Comme le décrit la [Figure 13](#) à la page 51, l'interface utilisateur permet également de gérer les cellules Data Protector en toute transparence avec le Gestionnaire de cellule sur toutes les plates-formes prises en charge.



**Figure 13 Utilisation de l'interface utilisateur de Data Protector**

**💡 CONSEIL :**

Dans un environnement mixte classique, installez l'interface utilisateur de Data Protector sur plusieurs systèmes de l'environnement afin d'avoir accès à Data Protector à partir de ces systèmes.

## Interface utilisateur graphique de Data Protector

L'interface graphique Data Protector d'origine, décrite à la [Figure 14](#) à la page 52, ainsi que l'interface graphique Java de Data Protector, décrite à la [Figure 15](#) à la page 52, sont des outils puissants et faciles à utiliser, qui présentent les caractéristiques suivantes :

- Un onglet Résultats dans lequel figurent les propriétés, les listes et les assistants de configuration.
- La configuration et la gestion simples des sauvegardes d'applications de base de données en ligne fonctionnant dans les environnements Windows, telles que Microsoft SQL, Microsoft Exchange Server, SAP R/3 et Oracle, ou fonctionnant dans les environnements UNIX, telles que SAP R/3, Oracle et Informix Server.
- Un système d'aide en ligne complet qui comprend des rubriques d'aide et une aide contextuelle.

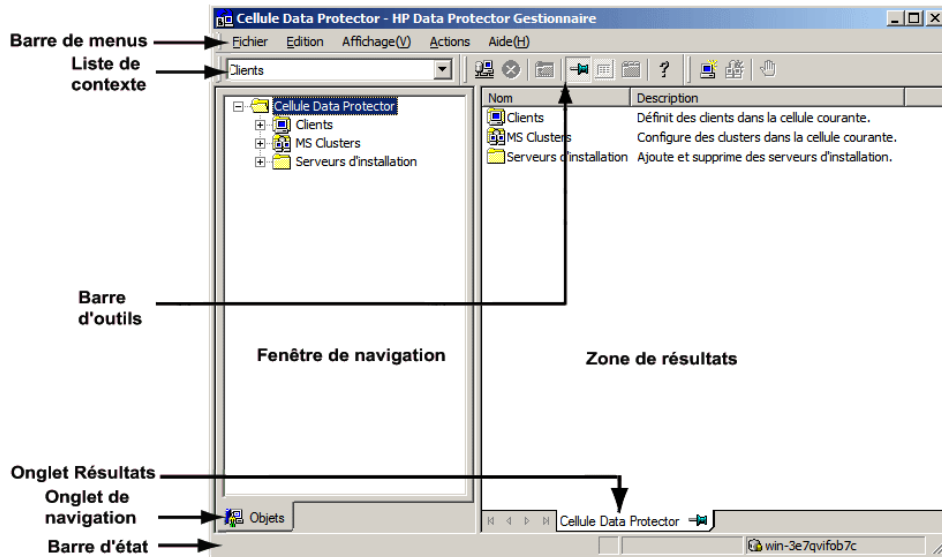


Figure 14 Interface graphique Data Protector d'origine

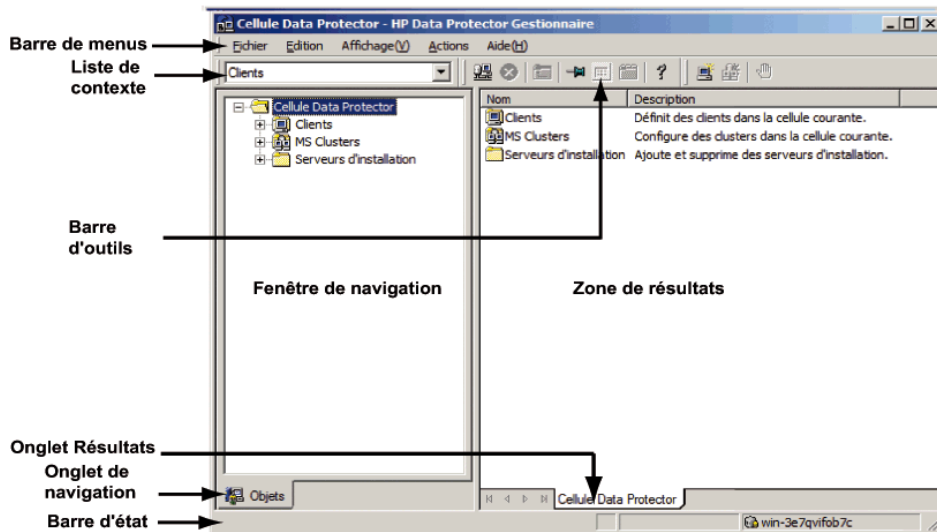
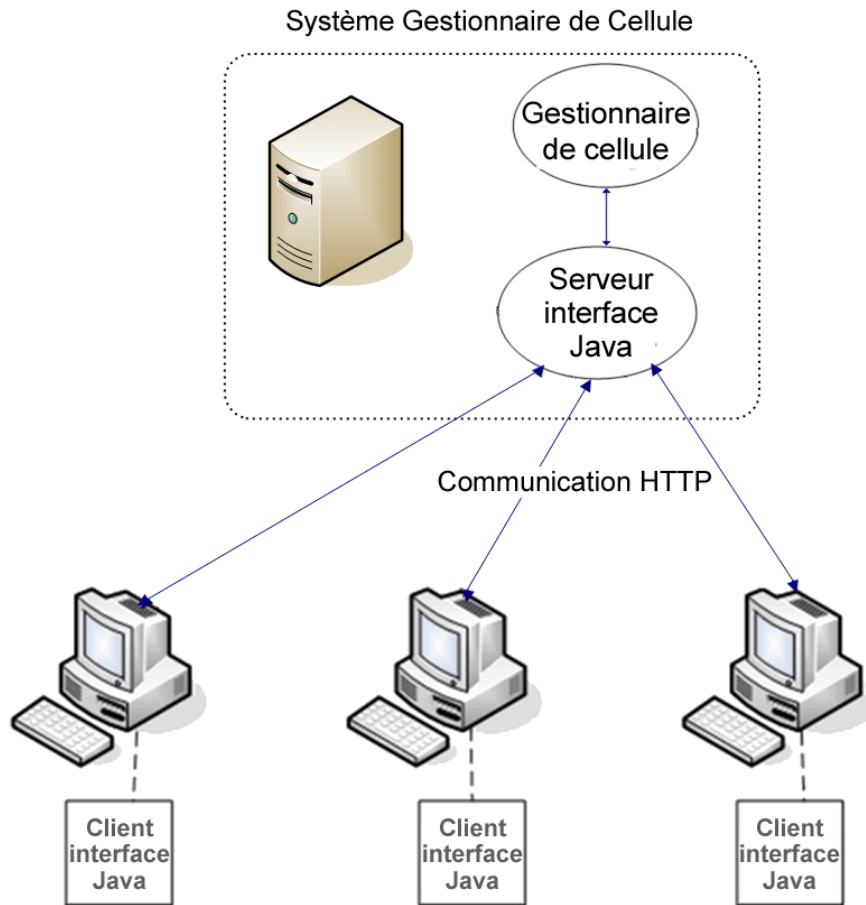


Figure 15 interface graphique Java de Data Protector

## Interface graphique Java de Data Protector

L'interface utilisateur graphique Java de Data Protector est une interface compatible Java basée sur une architecture client-serveur. Elle permet une gestion des sauvegardes avec la même richesse fonctionnelle que l'interface graphique Data Protector d'origine.

L'interface graphique Java se compose de deux éléments : serveur d'interface Java et client d'interface Java. La [Figure 16](#) à la page 53 indique la relation entre ces éléments.



**Figure 16 Architecture de l'interface graphique Java de Data Protector**

Le serveur d'interface Java est installé sur le système Gestionnaire de cellule Data Protector. Il reçoit et traite les requêtes du client de l'interface Java, puis renvoie les réponses au client de l'interface Java. Les données sont échangées via le protocole HTTP (Hypertext Transfer Protocol) sur le port 5556.

Le client d'interface Java ne dispose que de fonctions d'interface utilisateur et son fonctionnement exige une connexion au serveur d'interface Java.

## Avantages de l'interface Java

Par rapport à son interface graphique d'origine, l'interface graphique Java de Data Protector présente les avantages suivants :

- **Portabilité**  
L'architecture de l'interface graphique Java de Data Protector permet d'installer des clients d'interface Java sur toutes les plates-formes qui prennent en charge l'environnement JRE (Java Runtime Environment).
- **Configuration facile du pare-feu**  
Le client d'interface Java utilise le port 5556 pour la connexion au serveur d'interface Java. Il est plus facile de configurer l'interface graphique Java dans un environnement de pare-feu, car un seul port doit être ouvert. La communication entre le client d'interface Java et le serveur d'interface Java s'effectue au moyen du protocole HTTP, également plus convivial en termes de pare-feu.  
Pour plus d'informations, reportez-vous aux matrices de support Data Protector sous Specifications à l'adresse <http://www.hp.com/support/manuals>.
- **Localisation et internationalisation améliorées**  
Un seul package d'installation est nécessaire pour toutes les langues. L'interface Java assure un affichage plus performant dans toutes les langues, car les éléments sont redimensionnés automatiquement en fonction de la taille du texte.
- **Comportement non bloquant**  
Le serveur avec interface Java ne transmet que les données du contexte actif, ce qui réduit le trafic réseau entre le serveur Java et le client Java. Grâce à son comportement non bloquant, vous pouvez travailler sur différents contextes pendant que le serveur Java traite vos requêtes en arrière-plan.

## Différences par rapport à l'interface graphique Data Protector d'origine

En raison des spécificités des technologies de base utilisées, les deux interfaces graphiques présentent également certaines différences fonctionnelles mineures et visuelles. Ces différences n'ont que peu d'effet sur les fonctionnalités de Data Protector.

Par exemple, dans le contexte **Clients**, si vous affichez l'onglet **Sécurité** des propriétés d'un client, l'exploration du réseau fonctionne différemment selon l'interface utilisée :

- L'interface graphique Data Protector d'origine (sur les systèmes Windows uniquement) affiche le voisinage réseau du client d'interface.

- L'interface graphique Java de Data Protector affiche le voisinage réseau du Gestionnaire de cellule, et pas celui du client d'interface. L'exploration n'est possible qu'avec un Gestionnaire de cellule Windows. Cependant, l'interface peut s'exécuter sur un système Windows ou UNIX.

## Présentation des tâches nécessaires à la configuration de Data Protector

Vous trouverez dans cette section un aperçu général des tâches à effectuer pour configurer votre environnement de sauvegarde Data Protector. Selon la taille et la complexité de votre environnement, vous n'aurez pas forcément besoin de suivre toutes ces étapes.

1. Analysez la structure de votre réseau et de votre organisation. Déterminez les systèmes qui devront être sauvegardés.
2. Déterminez si vous souhaitez sauvegarder des applications et des bases de données spéciales, telles que Microsoft Exchange, Oracle, IBM DB2 UDB, SAP R/3 ou autres. Data Protector propose des intégrations spécifiques pour ces produits.
3. Décidez de la configuration de votre cellule Data Protector, notamment :
  - le système à définir comme Gestionnaire de cellule
  - les systèmes sur lesquels vous souhaitez installer l'interface utilisateur
  - la sauvegarde locale/sauvegarde réseau
  - les systèmes qui devront contrôler les périphériques et bibliothèques de sauvegarde
  - le type des connexions : LAN et/ou SAN
4. Achetez les licences Data Protector requises pour votre configuration. Vous pourrez ainsi obtenir les mots de passe que vous devez installer.

Vous pouvez également utiliser Data Protector à l'aide d'un mot de passe temporaire. Celui-ci n'est cependant valable que pendant 60 jours à compter de la date d'installation. Pour plus d'informations, reportez-vous au *Guide d'installation et de choix des licences HP Data Protector*.

5. Tenez compte des aspects ayant trait à la sécurité :
  - Analysez les questions liées à la sécurité. Reportez-vous au *Guide d'installation et de choix des licences HP Data Protector*.
  - Tenez compte des groupes d'utilisateurs à configurer.
  - Renforcez la sécurité en écrivant les données sur un support au format crypté.
  - Empêchez tout accès non autorisé en activant les communications de contrôle cryptées.
6. Décidez de la structure de vos sauvegardes :
  - Quels pools de supports seront utilisés et de quelle manière ?
  - Quels périphériques seront utilisés et de quelle manière ?
  - Combien de copies de chaque sauvegarde souhaitez-vous ?
  - De combien de spécifications de sauvegarde avez-vous besoin et comment ces dernières devront-elles être regroupées ?
  - Si vous comptez faire une sauvegarde sur disque, pensez aux stratégies de sauvegarde avancées telles que la sauvegarde synthétique et la sauvegarde de disque en plusieurs étapes.
7. Installez et configurez votre environnement Data Protector.
  - Installez le système du Gestionnaire de cellule Data Protector et utilisez l'interface utilisateur de Data Protector pour distribuer les composants Data Protector sur d'autres systèmes.
  - Connectez les périphériques (lecteurs de bande) aux systèmes qui devront les contrôler.
  - Configurez les périphériques de sauvegarde.
  - Configurez les pools de supports et préparez les supports.
  - Configurez les spécifications de sauvegarde, notamment la sauvegarde de l'IDB.
  - Le cas échéant, configurez les rapports.
8. Familiarisez-vous avec les tâches suivantes :
  - Gestion des échecs de sauvegarde
  - Exécution des opérations de restauration
  - Duplication des données sauvegardées et mise au coffre des supports
  - Préparation de la récupération après sinistre
  - Gestion de la base IDB



---

# 2 Planification de la stratégie de sauvegarde

## Dans ce chapitre

Ce chapitre traite de la planification d'une stratégie de sauvegarde. Il étudie en particulier la planification des cellules Data Protector, les performances et la sécurité, ainsi que la sauvegarde et la restauration des données. Il couvre en outre les types de sauvegarde de base, les opérations de sauvegarde automatisées, la gestion des clusters et la récupération après sinistre.

Il s'organise comme suit :

“Planification d'une stratégie de sauvegarde” à la page 58

“Planification de cellules” à la page 63

“Analyse et planification des performances” à la page 69

“Planification de la sécurité” à la page 76

“Gestion de clusters” à la page 85

“Sauvegardes complètes et incrémentales” à la page 98

“Conservation des données sauvegardées et des informations sur les données” à la page 106

“Sauvegarde de données” à la page 110

“Opération automatisée ou sans surveillance” à la page 119

“Duplication de données sauvegardées” à la page 121

“Vérification des supports et des objets de sauvegarde” à la page 136

“Restauration des données” à la page 138

“Récupération après sinistre” à la page 143

# Planification d'une stratégie de sauvegarde

Data Protector est simple à configurer et administrer. Toutefois, si vous travaillez dans un grand environnement comportant plusieurs systèmes client et que vous devez sauvegarder de très grandes quantités de données, il est préférable de planifier cette opération à l'avance. Cela simplifie la procédure de configuration ultérieure.

## Qu'est-ce que la planification d'une stratégie de sauvegarde ?

La planification d'une stratégie de sauvegarde est un processus qui comporte les étapes suivantes :

1. La définition des contraintes et des besoins relatifs aux sauvegardes, notamment la fréquence à laquelle vos données doivent être sauvegardées, le fait que vous ayez besoin ou non de copies supplémentaires des données sauvegardées sur des jeux de supports supplémentaires.
2. La maîtrise des facteurs qui influencent votre sauvegarde, notamment les taux de transfert de données pris en charge par le réseau et les périphériques de sauvegarde. Ces facteurs peuvent déterminer la manière dont vous configurez Data Protector et le type de sauvegarde (réseau ou directe par exemple) que vous choisissez. Par exemple, si vous utilisez la sauvegarde sur disque, vous pouvez bénéficier de stratégies de sauvegarde avancées telles que la sauvegarde synthétique et la sauvegarde de disque en plusieurs étapes.
3. La préparation d'une stratégie de sauvegarde décrivant votre concept de sauvegarde et sa mise en œuvre.

Vous trouverez dans cette section des informations détaillées sur les étapes décrites ci-dessus. Le reste de ce guide fournit des informations et remarques importantes, qui vous aideront à planifier votre sauvegarde.

## Définition des besoins relatifs à une stratégie de sauvegarde

La définition des objectifs et des contraintes de votre stratégie de sauvegarde implique de répondre aux questions suivantes :

- Quelle est la **politique de votre entreprise** en matière de sauvegarde et de restauration ?

Certaines entreprises ont une stratégie d'archivage et de stockage des données déjà définie. Il importe que votre stratégie de sauvegarde en tienne compte.

- Quels types de données sauvegarder ?

Etablissez une liste des types de données existants sur votre réseau, tels que les fichiers utilisateur, les fichiers système, les serveurs Web et les bases de données relationnelles volumineuses.

- Quel est le temps d'indisponibilité maximal à ne pas dépasser pour la récupération ?

Le temps d'indisponibilité autorisé a un impact important sur le choix des investissements en termes d'infrastructure réseau et de matériel de sauvegarde. Pour chaque type de données, déterminez le temps d'indisponibilité maximal acceptable pour la récupération ; en d'autres termes, déterminez, par type de données, la durée maximale d'indisponibilité avant restauration à partir d'une sauvegarde. Les fichiers utilisateur, par exemple, peuvent être restaurés dans un délai de deux jours, alors que certaines données d'entreprise stockées dans une base de données volumineuse doivent être récupérées dans un délai de deux heures maximum.

Le temps de récupération correspond essentiellement au temps nécessaire pour accéder au support et pour procéder à la restauration des données sur les disques. La récupération d'un système complet demande plus de temps, car des étapes supplémentaires sont nécessaires. Pour plus de détails, reportez-vous à la section "[Récupération après sinistre](#)" à la page 143.

- Pendant combien de temps conserver les différents types de données ?

Pour chaque type de données, définissez pendant combien de temps ces dernières doivent être conservées. Par exemple, vous pouvez avoir besoin de conserver les informations sur les employés de l'entreprise pendant cinq ans, alors que les fichiers utilisateur peuvent être utiles pendant trois semaines seulement.

- Comment conserver et maintenir les supports contenant des données sauvegardées ?

Pour chaque type de données, définissez pendant combien de temps les données d'un support doivent être conservées dans un coffre (lieu sûr situé à l'extérieur de l'entreprise), si vous utilisez ce type de stockage sécurisé. Par exemple, s'il n'est pas nécessaire de mettre au coffre les fichiers utilisateur, les informations relatives aux commandes, quant à elles, peuvent y être conservées pendant cinq ans, avec une vérification de chaque support tous les deux ans.

- Sur combien de jeux de supports les données doivent-elles être écrites pendant la sauvegarde ?

Pendant la sauvegarde, songez à écrire les données critiques sur plusieurs jeux de supports afin d'améliorer la tolérance aux pannes des sauvegardes ou de procéder à une mise au coffre sur plusieurs sites. La mise en miroir d'objet augmente le temps nécessaire à la sauvegarde.

- Quel volume de données sauvegarder ?

Pour chaque type de données, définissez la quantité estimée de données à sauvegarder. Celle-ci a une incidence sur le temps nécessaire à la sauvegarde et vous guide dans votre choix de périphériques et de supports de sauvegarde adaptés à vos besoins.

- Quelle est la croissance future estimée du volume de données ?

Pour chaque type de données, procédez à une estimation de la croissance à venir. Vous pourrez alors choisir des solutions de sauvegarde durables. Par exemple, si votre entreprise envisage d'embaucher 100 employés, la quantité de données relatives aux utilisateurs et aux systèmes client augmentera en conséquence.

- Combien de temps peut prendre une sauvegarde ?

Estimez le temps nécessaire à chaque sauvegarde. Ce paramètre a une incidence directe sur la durée pendant laquelle les données sont disponibles à l'utilisation. Les fichiers utilisateur peuvent être sauvegardés à tout moment, dès lors que les utilisateurs n'ont pas besoin d'y accéder. La disponibilité de certaines bases de données transactionnelles pour la sauvegarde peut, quant à elle, être limitée à quelques heures seulement.

Le temps nécessaire à la sauvegarde dépend du type de sauvegarde effectuée (complète ou incrémentale). Pour en savoir plus, reportez-vous à la section "[Sauvegardes complètes et incrémentales](#)" à la page 98. Data Protector permet également de sauvegarder certaines applications courantes de base de données en ligne. Pour plus d'informations, reportez-vous au *Guide d'intégration HP Data Protector*.

Si vous utilisez la sauvegarde sur disque, vous pouvez bénéficier de la sauvegarde synthétique et de la sauvegarde de disque en plusieurs étapes. Ces stratégies de sauvegardes avancées permettent de réduire considérablement le temps nécessaire à la sauvegarde. Pour plus d'informations, reportez-vous au [Chapitre 10](#) à la page 275 et à la section [Sauvegarde de disque en plusieurs étapes](#) à la page 128.

Si vous devez sauvegarder les données d'un disque très rapide et de grande capacité sur un périphérique plus lent, rappelez-vous que vous avez la possibilité d'utiliser plusieurs Agents de disques simultanément. Le lancement simultané de plusieurs Agents de disque sur un même disque permet d'accélérer considérablement les performances de sauvegarde.

- A quelle fréquence sauvegarder les données ?

Pour chaque type de données, indiquez la fréquence de sauvegarde de vos données. Par exemple, les fichiers de travail des utilisateurs peuvent être sauvegardés quotidiennement, les données système chaque semaine et certaines transactions de base de données deux fois par jour.

## Facteurs influant sur votre stratégie de sauvegarde

Un certain nombre de facteurs influencent la manière dont votre stratégie de sauvegarde sera mise en œuvre. Il est important de bien les comprendre avant d'élaborer votre stratégie de sauvegarde. Ces facteurs sont les suivants :

- La politique et les besoins de votre entreprise en matière de sauvegarde et de stockage des données.
- La politique et les besoins de votre entreprise en matière de sécurité.
- La configuration physique de votre réseau.
- Les ressources informatiques et humaines disponibles sur les différents sites de votre entreprise.

## Préparation d'un plan de stratégie de sauvegarde

La planification aboutit à la définition d'une stratégie de sauvegarde qui doit prendre en compte les points suivants :

- Importance de la disponibilité des données du système (et de la sauvegarde) pour l'entreprise :
  - Nécessité de conserver les données sauvegardées à un emplacement distant en cas de sinistre
  - Niveau de continuité des opérations  
Cela comprend notamment un plan de récupération et de restauration pour l'ensemble des systèmes client stratégiques.
  - Sécurité des données sauvegardées  
Nécessité de contrôler l'accès aux locaux, afin d'en interdire l'entrée à toute personne non autorisée. Cela comprend également la protection des données pertinentes contre tout accès non autorisé, à l'aide de dispositifs physiques et d'une protection électronique par mot de passe.
- Types de données à sauvegarder  
Déterminez les différents types de données utilisés par votre entreprise et la manière dont vous souhaitez les combiner dans les spécifications de sauvegarde, ainsi que leurs périodes de disponibilité respectives pour les sauvegardes. Vous pouvez regrouper les données en catégories, telles que Données commerciales, Données de ressources de l'entreprise, Données de projet et Données personnelles, chaque catégorie ayant des besoins spécifiques.
- Mise en œuvre de la stratégie de sauvegarde

- Comment les sauvegardes sont-elles effectuées et quelles sont les options de sauvegarde utilisées ?

Ces critères permettent de définir la fréquence des sauvegardes complètes et incrémentales, les options de sauvegarde à utiliser, si les données sauvegardées doivent ou non être protégées définitivement et si les supports utilisés pour la sauvegarde doivent ou non être confiés à une société chargée de les protéger.

- Comment regrouper les systèmes client dans des spécifications de sauvegarde ?  
Etudiez la meilleure manière de regrouper les spécifications de sauvegarde (par service, type de données ou fréquence de sauvegarde).

- Comment planifier les sauvegardes ?

Pensez à utiliser une approche échelonnée, selon laquelle les sauvegardes complètes des divers clients (spécifications de sauvegarde) se déroulent à des dates différentes afin d'éviter les problèmes liés à une surcharge du réseau, à une surcharge des périphériques et à la fenêtre temporelle.

- Comment conserver les données stockées sur les supports et les informations concernant les sauvegardes ?

Pensez à protéger les données pendant une période spécifique contre tout risque d'écrasement lors de nouvelles sauvegardes. Cette période de protection, appelée "protection des données", doit être définie lors de chaque session.

Définissez la période pendant laquelle la base de données catalogue doit conserver les informations sur les versions de sauvegarde, le nombre de fichiers et de répertoires sauvegardés et les messages stockés dans la base de données. Les données sauvegardées sont facilement accessibles tant que cette protection de catalogue est en vigueur.

- Configuration des périphériques

Déterminez les périphériques à utiliser pour les sauvegardes et les systèmes client auxquels ils sont connectés. Connectez les périphériques de sauvegarde aux systèmes client comportant les plus grandes quantités de données, afin de sauvegarder localement le plus de données possible plutôt que via le réseau. Vous accélerez ainsi la vitesse de sauvegarde.

Si vous avez besoin de sauvegarder d'importantes quantités de données :

- Envisagez l'utilisation d'un périphérique de bibliothèque.
- Envisagez l'utilisation d'un périphérique sur disque pour vos sauvegardes. La sauvegarde sur disque présente de nombreux avantages, elle permet notamment de réduire le temps nécessaire à la sauvegarde et l'utilisation de stratégies telles que la sauvegarde synthétique et la sauvegarde de disque en plusieurs étapes.

- Gestion des supports  
Déterminez le type de support à utiliser, ainsi que la manière de regrouper les supports en pools et de placer les objets sur ces supports.  
Déterminez le mode d'utilisation des supports dans le cadre des stratégies de sauvegarde.
- Mise au coffre  
Déterminez si les supports doivent être stockés dans un lieu sûr (un coffre) où ils seront conservés durant une période déterminée. Dans cette optique, songez à dupliquer les données sauvegardées pendant ou après la sauvegarde.
- Administrateurs et opérateurs de sauvegarde  
Déterminez les droits des utilisateurs chargés d'administrer et d'utiliser votre produit de stockage.

## Planification de cellules

L'un des choix les plus importants en ce qui concerne la planification de votre stratégie de sauvegarde consiste à savoir si vous souhaitez utiliser un environnement à une ou plusieurs cellules. Dans cette section, nous allons décrire :

- Les facteurs à prendre en considération lors de la planification de cellules
- Comment les cellules sont rattachées à un environnement réseau type
- La manière dont les cellules sont liées aux domaines Windows
- Comment les cellules sont rattachées aux environnements de groupes de travail Windows

## Une ou plusieurs cellules ?

Avant de décider si vous allez utiliser un environnement à une ou plusieurs cellules, considérez les éléments suivants :

- Problèmes liés à l'administration des sauvegardes  
L'utilisation d'un environnement à cellules multiples vous permet de bénéficier d'une plus grande liberté d'administration au sein de chaque cellule. Vous pouvez appliquer à chaque cellule une stratégie de gestion des supports indépendante. Si vous avez plusieurs groupes d'administration, vous pouvez, pour des raisons de sécurité, ne pas souhaiter qu'une cellule chevauche ces groupes. L'utilisation d'un environnement comportant plusieurs cellules peut présenter des désavantages (travail d'administration plus important, voire nécessité de définir un administrateur différent pour chaque cellule).

- **Taille des cellules**  
La taille d'une cellule Data Protector a une influence sur les performances de la sauvegarde et sur la capacité à gérer la cellule. La taille maximale recommandée pour une cellule Data Protector est de 100 systèmes client. Les cellules comportant plus de 200 systèmes client sont moins faciles à gérer.
- **A propos du réseau**  
Pour des performances optimales, tous les systèmes client d'une cellule doivent se trouver sur le même réseau local. Reportez-vous aux sections suivantes pour plus d'informations sur les autres points à prendre en considération concernant le réseau, notamment la configuration réseau.
- **Emplacement géographique**  
Si les systèmes client à sauvegarder se trouvent sur des sites distants, il peut être difficile de les gérer à partir d'une seule cellule et des problèmes réseau peuvent se produire entre les systèmes client. En outre, la sécurité des données peut poser problème.
- **Fuseaux horaires**  
Chaque cellule doit se trouver dans un fuseau horaire donné.
- **Sécurité des données**  
Dans Data Protector, la sécurité des données est définie au niveau de chaque cellule. Tout le travail d'administration de Data Protector s'effectue dans le cadre d'une seule cellule : les supports, les périphériques de sauvegarde et les données sauvegardées appartiennent à une seule cellule. Notez que Data Protector permet de partager des périphériques ou de déplacer des supports entre plusieurs cellules ; l'accès physique aux supports doit donc être sécurisé et limité au seul personnel autorisé.
- **Environnements mixtes**  
Data Protector vous permet de sauvegarder dans une même cellule des systèmes client de plates-formes différentes. Toutefois, il peut être pratique de regrouper dans une cellule les systèmes client partageant une même plate-forme. Par exemple, les systèmes client Windows peuvent être regroupés dans une cellule et les clients UNIX dans une autre. Cela est particulièrement utile si vous avez défini des stratégies et des administrateurs distincts pour chacun des environnements UNIX et Windows.
- **Services et sites**  
Vous pouvez regrouper chaque service ou site dans une cellule propre, par exemple en définissant une cellule pour le service comptabilité, une pour le service informatique et une autre pour le service production. Même si vous optez pour



une organisation comportant plusieurs cellules, Data Protector vous permet de configurer facilement des stratégies communes pour les différentes cellules.

## Installation et maintenance des systèmes client

Si vous utilisez plusieurs systèmes client UNIX et Windows, il est essentiel que vous ayez un dispositif efficace pour l'installation de Data Protector. Une installation locale sur chaque client n'est pas réalisable dans les grands environnements.

### Serveur d'installation et Gestionnaire de cellule

Le système principal d'une cellule Data Protector est le Gestionnaire de cellule. Pour pouvoir distribuer (installer à distance) correctement les composants Data Protector sur les systèmes client à partir d'un emplacement central, un système contenant le référentiel du logiciel Data Protector est nécessaire. Ce système est appelé Serveur d'installation Data Protector. Par défaut, le Gestionnaire de cellule est également un Serveur d'installation.

Chaque fois que vous effectuez une installation à distance, vous devez accéder au Serveur d'installation. L'utilisation d'un Serveur d'installation présente un avantage majeur : celui de réduire considérablement, surtout dans les environnements d'entreprise, le temps nécessaire à l'installation, la mise à jour, la mise à niveau et la désinstallation à distance du logiciel Data Protector.

Avant d'installer le logiciel, vous devez vous assurer que chaque Serveur d'installation et chaque Gestionnaire de cellule répond à certaines exigences matérielles et logicielles. Un port dédié (généralement le port 5555) doit être disponible pour l'ensemble de la cellule. Pour plus d'informations, reportez-vous au *Guide d'installation et de choix des licences HP Data Protector*.

L'installation d'un Gestionnaire de cellule et d'un Serveur d'installation se fait directement à partir du CD. Une fois ces systèmes installés, vous pouvez procéder à l'installation des composants sur divers systèmes client à l'aide de l'interface d'installation de Data Protector.

Lorsque vous installez initialement Data Protector, il s'exécute avec une licence temporaire valable pendant 60 jours ; vous pouvez ainsi utiliser Data Protector pendant deux mois sans posséder de licence permanente, ce qui vous laisse le temps de vous procurer les licences dont vous avez besoin.

Ainsi, pendant cette période, nous vous recommandons d'installer et de configurer votre environnement Data Protector, puis de demander votre licence permanente. Pour obtenir un mot de passe permanent, vous devez savoir à quelles cellules Data Protector appartiennent les différents systèmes client, connaître le nombre de

périphériques connectés aux systèmes client et savoir si vous avez besoin de certaines intégrations Data Protector.

## Création de cellules dans l'environnement UNIX

La création de cellules dans l'environnement UNIX est facile. Aidez-vous des considérations de ce guide pour déterminer les systèmes client à ajouter à la cellule et définir le système du Gestionnaire de cellule. Lors de l'installation, un accès au compte "root" de chaque système client est requis. Un système cohérent d'attribution de nom aux nœuds constitue un prérequis indispensable afin que chaque système client soit accessible à partir de tous les autres grâce à un même nom de nœud complet.

## Création de cellules dans l'environnement Windows

En raison des différentes configurations possibles (domaine/groupe de travail), les différents niveaux de support des administrateurs Windows peuvent avoir un impact sur la configuration de Data Protector pendant l'installation. Un système cohérent d'attribution de nom aux nœuds est une condition préalable indispensable afin que chaque système client soit accessible à partir de tous les autres grâce à un même nom de nœud complet.

## Domaines Windows

Vous pouvez facilement mettre en correspondance un domaine Windows avec une cellule Data Protector. Dans un domaine Windows unique, utilisez un mappage un à un si la taille du domaine ne dépasse pas celle recommandée pour la cellule Data Protector. Sinon, séparez le domaine en plusieurs cellules et gérez ces dernières à l'aide du Manager-of-Managers Data Protector.

## Mise en correspondance d'une cellule Data Protector dans un domaine Windows

La mise en correspondance d'une cellule Data Protector dans un domaine Windows permet également de simplifier le processus d'administration au sein de Data Protector lui-même. Pour cela, distribuez le logiciel de sorte que tous les systèmes client puissent être installés à l'aide d'un compte Windows central dans une organisation par domaine. Toutefois, les autres opérations ne sont pas limitées à une organisation par domaine Windows, car toutes les opérations et vérifications de sécurité sont réalisées par le protocole interne de Data Protector et non par le dispositif de sécurité de Windows.

D'une manière générale, il n'existe aucune restriction quant à la manière d'installer Data Protector et au choix de son emplacement d'installation. Toutefois, en raison de la structure de Windows et des configurations les plus courantes, qui sont des environnements avec domaines, certaines opérations sont plus faciles à réaliser lorsque Data Protector est mis en correspondance avec un modèle de domaine unique ou avec un modèle de domaines multiples dont l'un est le domaine principal ; ainsi un seul utilisateur peut gérer l'ensemble des systèmes client à l'intérieur de l'environnement (distribution logicielle et configuration utilisateur).

Cette question prend toute son importance dans un environnement multicellule utilisant un Manager-of-Managers, car toutes les cellules configurées nécessitent un administrateur central ayant accès à la totalité de l'environnement de sauvegarde. Lorsqu'un seul domaine est configuré, ou plusieurs avec un domaine principal, l'utilisateur du domaine principal global peut aussi être l'administrateur de l'ensemble des cellules et de l'environnement Manager-of-Managers. Si vous utilisez plusieurs domaines indépendants, vous devez configurer plusieurs utilisateurs pour administrer l'environnement.

## Groupes de travail Windows

Certaines tâches de configuration sont plus longues à effectuer car il n'y a pas d'utilisateur global comme c'est le cas dans un domaine. La distribution logicielle nécessite un nom de connexion unique pour chaque système client sur lequel le logiciel est installé. En d'autres termes, pour installer 100 systèmes client dans un environnement de groupes de travail, vous devez entrer 100 noms de connexion. Dans ce cas, nous vous recommandons d'utiliser un environnement de domaines ; en effet, les tâches d'installation et un grand nombre d'autres tâches d'administration non liées à Data Protector sont beaucoup plus faciles à effectuer dans les grands environnements.

Pour utiliser le MoM (Manager-of-Managers) dans ce type d'environnement, vous devez configurer séparément l'administrateur pour chaque cellule, afin de pouvoir gérer l'environnement MoM depuis n'importe quelle cellule.

Là encore, Data Protector n'est pas limité à une organisation Windows par domaine. Toutefois, cette organisation permet de tirer parti des procédures d'administration nécessitant l'authentification de l'utilisateur (installation, gestion des utilisateurs par exemple), et de les simplifier.

## Création de cellules dans un environnement mixte

Si vous travaillez dans un environnement mixte, nous vous recommandons de tenir compte des facteurs décrits à la section "[Création de cellules dans l'environnement UNIX](#)" à la page 66. Plus un environnement comporte de domaines et de groupes

de travail, plus le nombre de comptes à créer et d'étapes à suivre est important pour distribuer le logiciel et préparer l'environnement à l'administration.

## Cellules distantes géographiquement

Data Protector vous permet d'administrer facilement les cellules géographiquement distantes. Pour plus de détails, reportez-vous à la section "[Séparation d'un environnement en plusieurs cellules](#)" à la page 45.

### A propos des cellules géographiquement distantes

Lorsque vous configurez des cellules géographiquement distantes, rappelez-vous ce qui suit :

- Les données ne sont pas envoyées via un WAN.  
Les périphériques et les systèmes client que vous sauvegardez sont configurés localement.
- Les cellules sont configurées dans un MoM.  
Pour gérer de manière centralisée les cellules distantes géographiquement, vous devez les configurer dans un environnement MoM.
- Analysez les configurations utilisateur.  
Vous devez prendre en compte tous les points que nous avons mentionnés au sujet des configurations à domaine unique, à domaines multiples et par groupe de travail.

Vous pouvez configurer une seule cellule recouvrant plusieurs emplacements distants géographiquement. Pour cela, vous devez vous assurer que le transfert des données depuis chaque système client vers le périphérique correspondant n'est pas effectué par le biais d'un WAN. En effet, les connexions par réseau WAN n'étant pas stables, vous risquez de les perdre.

### Environnement MoM

Un environnement MoM ne requiert pas de connexion réseau fiable entre les cellules et la cellule centrale MoM, car seuls les contrôles sont envoyés via les connexions longue distance et les sauvegardes sont effectuées en local dans chaque cellule Data Protector. Cela présuppose en revanche que chaque cellule dispose de sa propre base de données de gestion des supports.

Dans ce cas, utilisez l'option de sauvegarde **Reconnecter les connexions rompues** de Data Protector pour rétablir les connexions interrompues.

# Analyse et planification des performances

Dans les environnements stratégiques, il est indispensable de réduire le temps nécessaire à la récupération des données en cas d'altération de la base de données ou d'une panne de disque. Il est donc extrêmement important d'analyser et de planifier les performances de sauvegarde. L'optimisation du temps nécessaire pour sauvegarder un grand nombre de systèmes client et de bases de données volumineuses, tous connectés à des plates-formes et à des réseaux différents, est une tâche complexe.

Vous trouverez dans les sections suivantes un aperçu des facteurs de performances de sauvegarde les plus courants. En raison du grand nombre de variables existantes, il nous est impossible de donner des recommandations tenant compte de l'ensemble des besoins des utilisateurs.

## Infrastructure

L'infrastructure a un impact important sur les performances de sauvegarde et de restauration. Les aspects les plus importants sont le parallélisme des chemins d'accès aux données et l'utilisation de matériel rapide.

## Sauvegarde locale ou réseau

L'envoi de données sur le réseau ajoute un paramètre supplémentaire, le réseau ayant un effet sur les performances. Data Protector gère le flux de données différemment dans les cas suivants :

- Flux de données sur un réseau : du disque vers la mémoire du système source, vers le réseau, vers la mémoire du système de destination, vers le périphérique
- Flux de données en local : du disque vers la mémoire vers le périphérique

Pour optimiser les performances avec les flux de données importants, utilisez les configurations de sauvegarde locale.

## Périphériques

### Performances des périphériques

Le type et le modèle du périphérique ont une influence sur ses performances en raison de la vitesse soutenue à laquelle le périphérique peut écrire des données sur une bande (ou les lire).

Les taux de transfert de données atteints dépendent également de l'utilisation de la compression matérielle. Le taux de compression réalisable dépend de la nature des données sauvegardées. Dans la plupart des cas, l'utilisation de périphériques rapides et de la compression matérielle permet d'améliorer les performances obtenues. Toutefois, cela n'est vrai que si les périphériques fonctionnent en mode continu.

Au démarrage ou à la fin d'une session de sauvegarde, les périphériques de sauvegarde ont besoin d'un peu de temps pour effectuer des opérations telles que le rembobinage des supports, le montage ou le démontage des supports.

Les bibliothèques offrent des avantages supplémentaires grâce à leur accès rapide et automatisé à un grand nombre de supports. Au moment de la sauvegarde, le chargement d'un nouveau support ou d'un support réutilisable est requis. En outre, le support contenant les données à restaurer doit être accessible rapidement au moment de la restauration.

L'accès aux données des périphériques sur disque est plus rapide qu'avec des périphériques conventionnels car aucun chargement/déchargement des supports n'est nécessaire. Les délais de sauvegarde et de restauration en sont donc réduits. De plus, avec les périphériques sur disque, il est possible d'utiliser des stratégies de sauvegarde avancées telles que la sauvegarde synthétique et la sauvegarde de disque en plusieurs étapes, ce qui réduit également le temps nécessaire aux opérations de sauvegarde et de restauration.

## Matériel hautes performances autre que les périphériques

### Performances des systèmes informatiques

La vitesse de fonctionnement des systèmes informatiques a un impact direct sur les performances. Lors des sauvegardes, les systèmes sont chargés par la lecture des disques, la compression logicielle, etc.

Le taux de données lues sur disque et le taux d'utilisation du processeur sont des critères de performances importants pour les systèmes eux-mêmes, en plus des performances d'E/S et du type de réseau utilisé.

## Configuration hautes performances avancée

La solution de sauvegarde avec temps d'indisponibilité nul (Zero Downtime Backup, ZDB) de Data Protector permet de réduire le temps d'indisponibilité des applications ou la durée du mode sauvegarde et de diminuer la charge du réseau en utilisant les périphériques de sauvegarde connectés en local à la place des périphériques de sauvegarde réseau. Le temps d'indisponibilité des applications ou la durée du mode sauvegarde se limite au temps de création de la réplique des données. Cette dernière

est ensuite sauvegardée via un système de sauvegarde sur un périphérique connecté en local.

Pour plus d'informations sur la sauvegarde avec temps d'indisponibilité nul, reportez-vous au *Guide conceptuel ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

## Utilisation en parallèle du matériel

L'utilisation en parallèle de plusieurs chemins d'accès aux données constitue une méthode fondamentale et efficace pour améliorer les performances. Cela comprend l'infrastructure réseau. Le parallélisme permet d'améliorer les performances dans les cas suivants :

### Cas d'utilisation du parallélisme

- Lorsque plusieurs systèmes client peuvent être sauvegardés localement, c'est-à-dire lorsque les disques et périphériques associés sont connectés au même système client.
- Lorsque plusieurs systèmes client peuvent être sauvegardés sur le réseau. Dans ce cas, l'acheminement du trafic réseau doit permettre d'éviter que les chemins d'accès aux données ne se chevauchent. Dans le cas contraire, les performances seront réduites.
- Lorsque plusieurs objets (disques) peuvent être sauvegardés sur un ou plusieurs périphériques (à bandes).
- Lorsque plusieurs liens réseau dédiés entre des systèmes client peuvent être utilisés. Par exemple, si 6 objets (disques) doivent être sauvegardés sur système\_A et que système\_B dispose de 3 périphériques à bandes rapides, vous pouvez utiliser 3 liens réseau dédiés entre système\_A et système\_B.
- Partage de charge

Cette option permet à Data Protector de déterminer de manière dynamique les périphériques sur lesquels les objets (disques) doivent être sauvegardés. Activez cette fonctionnalité, en particulier lorsque vous devez sauvegarder un grand nombre de systèmes de fichiers dans un environnement dynamique. Pour plus de détails, reportez-vous à la section "[Fonctionnement du partage de charge](#)" à la page 173.

Remarque : vous ne pouvez toutefois pas prévoir sur quels supports un objet donné sera écrit.

## Configuration des sauvegardes et des restaurations

Toute infrastructure doit être utilisée de manière à optimiser les performances du système. Data Protector est un outil très flexible capable de s'adapter à votre environnement et à la manière dont vous souhaitez effectuer vos sauvegardes et vos restaurations.

### Compression logicielle

L'UC du client effectue une compression logicielle lors de la lecture des données d'un disque. Ce procédé permet de réduire le volume des données envoyées sur le réseau, mais nécessite que le client dispose de ressources UC importantes.

La compression logicielle est désactivée par défaut. Vous ne devez utiliser la compression logicielle que pour sauvegarder les données d'un grand nombre de machines sur un réseau lent, et lorsque les données peuvent être compressées avant d'être envoyées sur le réseau. Pensez à désactiver la compression matérielle lorsque vous utilisez la compression logicielle, deux opérations de compression ayant pour effet d'augmenter le volume des données.

### Compression matérielle

La compression matérielle s'effectue comme suit : un périphérique reçoit les données d'origine d'un serveur de lecteurs et les écrit sur des supports en mode compressé. 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.

La compression matérielle est activée par défaut. Sur les systèmes HP-UX, vous pouvez activer la compression matérielle en sélectionnant un fichier de périphérique de compression matérielle. Sur les systèmes Windows, vous devez l'activer lors de la configuration du périphérique. Utilisez cette option de compression avec précaution car les données écrites sur des supports en mode compressé *ne peuvent pas* être lues au moyen d'un périphérique fonctionnant en mode non compressé, et vice versa.

### Sauvegardes complètes et incrémentales

Une méthode simple pour améliorer les performances consiste à réduire la quantité de données à sauvegarder. Il est recommandé de planifier soigneusement vos sauvegardes complètes et incrémentales. Notez que vous n'avez pas nécessairement besoin d'effectuer simultanément toutes les sauvegardes complètes de l'ensemble des systèmes client.



Si vous utilisez la sauvegarde sur disque, vous pouvez utiliser des stratégies de sauvegarde avancées telles que la sauvegarde synthétique et la sauvegarde de disque en plusieurs étapes.

## Sauvegarde d'image disque ou sauvegarde de système de fichiers

S'il était auparavant plus efficace de sauvegarder des images disque (volumes bruts) plutôt que des systèmes de fichiers, cela n'est plus le cas aujourd'hui, à l'exception des systèmes fortement chargés ou des disques contenant un grand nombre de petits fichiers, par exemple. D'une manière générale, il est préférable d'utiliser la sauvegarde de systèmes de fichiers.

## Distribution des objets sur les supports

Voici quelques exemples de configurations de sauvegarde objet/support fournies par Data Protector :

- Un objet (disque) est stocké sur un support.  
L'avantage de cette méthode est qu'il existe une relation fixe connue entre un objet et un support, sur lequel l'objet réside. Cela peut être utile pour le processus de restauration car le système a ainsi besoin d'accéder à *un seul* support.  
Toutefois, cette méthode présente un inconvénient dans une configuration de sauvegarde en réseau. En effet, le réseau agit comme un facteur de limitation des performances du système, empêchant le périphérique de fonctionner en mode continu.
- De nombreux objets sont stockés sur un petit nombre de supports ; chaque support contient des données provenant de plusieurs objets ; un objet est stocké sur un périphérique.  
L'avantage de cette méthode tient à la flexibilité des flux de données au moment de la sauvegarde, ce qui participe à l'optimisation des performances, en particulier dans le cas d'une configuration en réseau.  
La stratégie présuppose que les périphériques, à chacun desquels parviennent simultanément des données émanant de plusieurs sources, reçoivent un flux de données suffisant pour fonctionner en mode continu.  
L'inconvénient de cette méthode tient à la perte de temps résultant du fait que les données (d'autres objets) sont ignorées lors de la restauration d'un objet spécifique. En outre, cette méthode ne permet pas de prévoir précisément sur quel support seront stockées les données d'un objet.  
Pour plus d'informations sur le mode de fonctionnement continu des périphériques et les sauvegardes simultanées, reportez-vous à la section "[Périphérique en mode continu et simultanéité](#)" à la page 173.

## Performances des disques

Toutes les données sauvegardées par Data Protector dans vos systèmes résident sur des disques. Les performances de ces disques ont donc une influence directe sur les performances de sauvegarde. Un disque est avant tout un périphérique séquentiel ; en d'autres termes, vous pouvez y lire ou y écrire des données, mais vous ne pouvez pas effectuer ces deux opérations simultanément. De même, vous ne pouvez lire ou écrire qu'un flux de données à la fois. Dans Data Protector, les systèmes de fichiers sont sauvegardés de manière séquentielle pour réduire les mouvements de la tête du disque. Les fichiers sont restaurés de la même manière.

Ce principe de fonctionnement n'est pas toujours observable, car le système d'exploitation stocke les données les plus utilisées dans la **mémoire cache**.

## Fragmentation des disques

Les données sur un disque ne sont pas stockées dans l'ordre logique où elles apparaissent lorsque vous parcourez les fichiers et les répertoires \*; elles sont fragmentées en petits blocs répartis sur l'ensemble du disque physique. Par conséquent, pour lire ou écrire un fichier, une tête de disque doit se déplacer sur l'ensemble de la surface du disque. Notez qu'il peut exister des différences d'un système d'exploitation à l'autre.



### CONSEIL :

Pour les fichiers volumineux, les sauvegardes sont plus efficaces lorsque les fichiers sont peu fragmentés.

---

## Compression

Si les données sont compressées sur un disque, le système d'exploitation Windows commence par les décompresser avant de les envoyer sur le réseau. Cela a pour conséquence de ralentir la vitesse de sauvegarde et d'utiliser beaucoup de ressources processeur.

## Sauvegardes d'image disque

Data Protector vous permet également de sauvegarder des disques UNIX sous forme d'images disque. En cas de sauvegarde d'image disque, une image de l'ensemble du disque est sauvegardée, sans suivre la structure du système de fichiers. La tête de disque se déplace de manière linéaire sur toute la surface du disque. La sauvegarde

d'image disque peut donc s'effectuer beaucoup plus rapidement que celle d'un système de fichiers.

## Performances de l'Agent de disque sur les systèmes Windows

Vous pouvez améliorer les performances de l'Agent de disque pour la sauvegarde de systèmes de fichiers Windows en activant la lecture asynchrone. La lecture asynchrone améliore les performances de l'Agent de disque lors de la sauvegarde de données sur des batteries de disque, en particulier quand des fichiers de grande taille sont traités. Il est recommandé d'effectuer des essais de sauvegarde afin de déterminer si la lecture asynchrone améliorera les performances dans votre environnement spécifique et de définir les paramètres appropriés pour une lecture asynchrone optimale.

## Performances SAN

Lorsque vous sauvegardez de gros volumes de données en une session, le temps nécessaire au transfert des données devient important. Il s'agit du temps requis pour déplacer les données vers un périphérique de sauvegarde, via une connexion (LAN, locale ou SAN).

## Performances des applications de base de données en ligne

Lorsque vous sauvegardez des bases de données et des applications, comme Oracle, SAP R/3, Sybase et Informix Server, les performances de sauvegarde dépendent également des applications. Les sauvegardes de base de données en ligne permettent à la sauvegarde de se dérouler alors que l'application de base de données reste en ligne. Cela permet d'optimiser la disponibilité de la base de données mais peut avoir un impact sur les performances de l'application. Data Protector s'intègre à toutes les applications courantes de base de données en ligne afin d'optimiser les performances de sauvegarde.

Reportez-vous au *Guide d'intégration HP Data Protector* pour plus d'informations sur l'intégration de Data Protector aux différentes applications et pour obtenir des conseils sur l'amélioration des performances de sauvegarde.

Consultez également la documentation fournie avec votre application de base de données en ligne pour plus d'informations sur l'amélioration des performances de sauvegarde.

# Planification de la sécurité

La sécurité des données est un facteur essentiel à prendre en compte lorsque vous planifiez votre environnement de sauvegarde. Un plan de sécurité soigneusement élaboré, mis en œuvre et mis à jour, vous permettra d'éviter tout accès, duplication ou modification non autorisé(e) à des données.

## Qu'est-ce que la sécurité ?

Dans le contexte de la sauvegarde, la sécurité consiste généralement à déterminer :

- qui peut administrer ou utiliser une application de sauvegarde (Data Protector) ;
- qui peut accéder physiquement aux systèmes client et aux supports de sauvegarde ;
- qui peut restaurer les données ;
- qui peut afficher les informations sur les données sauvegardées.

Data Protector vous propose des solutions de sécurité à tous ces niveaux.

## Fonctionnalités de sécurité Data Protector

Les fonctionnalités suivantes vous permettent d'autoriser et de limiter l'accès à Data Protector et aux données sauvegardées. Les éléments de la liste ci-dessous sont décrits en détail dans les sections suivantes.

- Cellules
- Comptes utilisateur Data Protector
- Groupes d'utilisateurs Data Protector
- Droits utilisateur Data Protector
- Visibilité et accès aux données sauvegardées
- Cryptage des données
- Communications de contrôle cryptées

## Cellules

### Démarrage de sessions

La sécurité Data Protector est basée sur les cellules. Les sessions de sauvegarde et de restauration ne peuvent être lancées qu'à partir du Gestionnaire de cellule, sauf si vous disposez de la fonctionnalité Manager-of-Managers de Data Protector. De

cette manière, les utilisateurs d'autres cellules ne peuvent ni sauvegarder, ni restaurer les données stockées dans les systèmes de votre cellule locale.

### Accès à partir d'un Gestionnaire de cellule spécifique

Data Protector vous permet en outre de définir explicitement le Gestionnaire de cellule à partir duquel un système client est accessible : en d'autres termes, de configurer un homologue certifié.

### Restriction pré- et post-exécution

Pour des raisons de sécurité, vous pouvez définir différents niveaux de restrictions pour les scripts pré- et post-exécution. Ces scripts facultatifs vous permettent de préparer un système client à la sauvegarde, par exemple, en fermant une application de manière à obtenir une sauvegarde cohérente.

## Comptes utilisateur Data Protector

Quiconque utilise une fonctionnalité de Data Protector, l'administre ou restaure des données personnelles, doit avoir un compte utilisateur Data Protector. Cela permet d'interdire tout accès non autorisé à Data Protector et aux données sauvegardées.

### Qui définit les comptes utilisateur ?

Un administrateur crée les comptes en indiquant un nom de connexion utilisateur et les systèmes à partir desquels l'utilisateur peut se connecter, et en l'affectant à un groupe d'utilisateurs Data Protector, lequel définit ses droits utilisateur.

### A quel moment les comptes sont-ils contrôlés ?

Lorsqu'un utilisateur démarre l'interface utilisateur Data Protector, Data Protector contrôle ses droits. Un contrôle a également lieu lorsqu'un utilisateur veut effectuer des tâches spécifiques.

Pour plus de détails, reportez-vous au [Chapitre 4](#) à la page 201.

## Groupes d'utilisateurs Data Protector

### Qu'est-ce qu'un groupe d'utilisateurs ?

Lorsqu'un compte utilisateur est créé, l'utilisateur devient membre du groupe d'utilisateurs spécifié. Pour chaque groupe, des droits utilisateur Data Protector

spécifiques ont été définis. Tous les membres du groupe disposent des droits définis pour le groupe.

### A quoi servent les groupes d'utilisateurs ?

Les groupes d'utilisateurs Data Protector simplifient la configuration des utilisateurs. L'administrateur peut regrouper les utilisateurs en fonction du type d'accès dont ils ont besoin. Par exemple, le groupe des utilisateurs finaux peut être autorisé uniquement à restaurer des données personnelles sur un système local, alors que le groupe des opérateurs sera autorisé à démarrer et à contrôler des sauvegardes, mais pas à en créer.

Pour plus de détails, reportez-vous au [Chapitre 4](#) à la page 201.

## Droits utilisateur Data Protector

### Que sont les droits utilisateur ?

Les droits utilisateur permettent de définir les actions qu'un utilisateur est autorisé à effectuer dans Data Protector. Ces droits sont définis au niveau du groupe d'utilisateurs de Data Protector et non pour chaque utilisateur individuellement. Les utilisateurs ajoutés à un groupe disposent automatiquement des droits qui lui sont attribués.

### A quoi servent les droits utilisateur ?

Data Protector dispose de fonctionnalités souples de gestion des utilisateurs et des groupes d'utilisateurs, qui permettent à l'administrateur de définir de manière sélective les utilisateurs pouvant accéder à une fonction Data Protector spécifique. Il est donc important de définir avec soin les droits utilisateur dans Data Protector : sauvegarder et restaurer des données revient plus ou moins à en faire une copie.

Pour plus de détails, reportez-vous au [Chapitre 4](#) à la page 201.

## Visibilité des données sauvegardées

Sauvegarder des données équivaut à en créer une copie. Il est donc indispensable, lorsque vous traitez des informations confidentielles, de limiter l'accès aux données d'origine et à celles de la sauvegarde.

### Interdiction d'accès aux données pour d'autres utilisateurs

Lorsque vous configurez une sauvegarde, vous devez décider si les données seront visibles par tous les utilisateurs (publiques) ou uniquement par le propriétaire de la sauvegarde (privées) au moment de la restauration. Pour plus d'informations,

reportez-vous à la section "Qu'est-ce que la propriété de sauvegarde ?" à la page 79.

## Qu'est-ce que la propriété de sauvegarde ?

### Qui est propriétaire d'une session de sauvegarde ?

Chaque session de sauvegarde et toutes les données sauvegardées sont affectées à un propriétaire. Le propriétaire peut être l'utilisateur qui démarre une sauvegarde interactive, le compte sous lequel le processus CRS s'exécute ou l'utilisateur désigné comme le propriétaire dans les options de la spécification de sauvegarde. Pour obtenir des instructions sur la procédure de désignation d'un propriétaire de sauvegarde, recherchez l'entrée suivante dans l'index de l'aide en ligne : "propriété".

### Propriété et restauration des sauvegardes

La propriété de sauvegarde influe sur la capacité des utilisateurs à consulter et à restaurer les données. A moins que l'objet ne soit défini comme public, seul le propriétaire du jeu de supports ou un administrateur est autorisé à voir les données stockées dans le jeu. Le droit de voir et de consulter des objets privés peut également être accordé à des groupes ne disposant pas de droits d'*administration*. Pour obtenir des instructions sur les droits de voir et de restaurer un objet privé et la manière de les appliquer, recherchez l'entrée suivante dans l'index de l'aide en ligne : "propriété".

## Cryptage des données

Les systèmes ouverts et l'utilisation de réseaux publics rendent la protection des données indispensable au sein des grandes entreprises. Data Protector vous permet de crypter les données sauvegardées de manière à les protéger vis à vis des autres. Deux techniques de cryptage des données sont disponibles dans Data Protector : le cryptage sur logiciel et le cryptage sur lecteur.

Le cryptage sur logiciel Data Protector, appelé **cryptage AES 256 bits**, est 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 leur transfert sur un réseau et leur écriture sur un support.

Data Protector Le **cryptage sur lecteur** utilise la fonctionnalité de cryptage du lecteur. La capacité réelle de mise en oeuvre et de cryptage dépend du microprogramme

du lecteur. Data Protector active simplement la fonctionnalité et gère les clés de cryptage.

La gestion des clés est assurée par le **serveur gestionnaire de clés (KMS)** qui se trouve sur le Gestionnaire de cellule Data Protector. Toutes les clés de cryptage sont stockées de manière centralisée dans le fichier de banque de clés sur le Gestionnaire de cellule et sont gérées par le serveur gestionnaire de clés (KMS).

Vous pouvez crypter tous les objets ou une sélection d'objets dans une spécification de sauvegarde, et également combiner les sessions cryptées ou non cryptées sur un même support.

Outre la fonctionnalité de cryptage, Data Protector propose également une fonctionnalité de codage qui utilise un algorithme intégré sans clé.

## Fonctionnement du cryptage AES 256 bits de Data Protector

Le Gestionnaire de session de sauvegarde (BSM) lit la spécification de sauvegarde dans laquelle l'option de cryptage **AES 256 bits** est sélectionnée et demande une clé de cryptage active auprès du serveur gestionnaire de clés (KMS). La clé est transférée à l'Agent de disque (DA) qui crypte les données. Les données sauvegardées sont donc cryptées avant d'être transférées sur un réseau et d'être écrites sur un support.

La [Figure 17](#) à la page 81 présente une interaction classique au cours d'une session de sauvegarde cryptée lorsque l'option de cryptage **AES 256 bits** est sélectionnée.



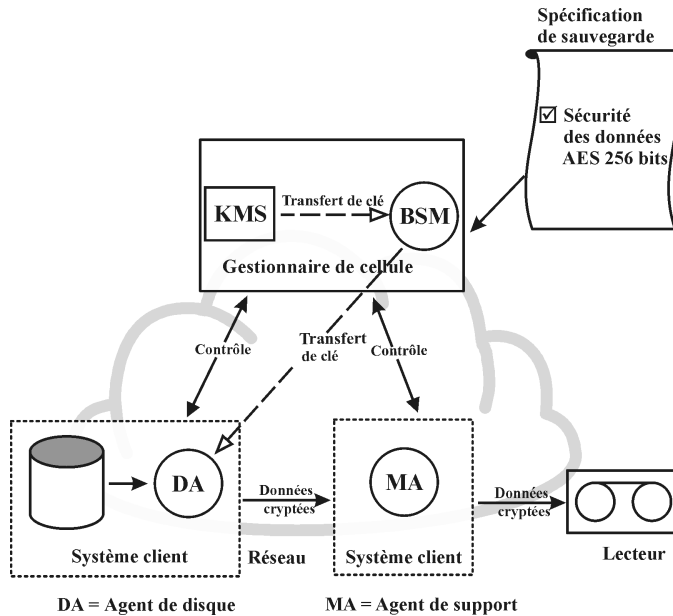


Figure 17 Session de sauvegarde avec cryptage AES 256 bits

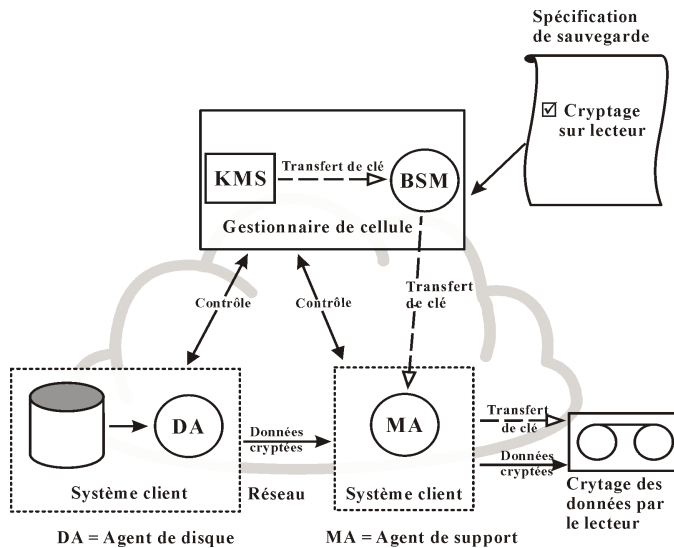
## Fonctionnement du cryptage sur lecteur de Data Protector

Le Gestionnaire de session de sauvegarde (BSM) lit la spécification de sauvegarde dans laquelle l'option **Cryptage sur lecteur** est sélectionnée et demande une clé de cryptage active auprès du serveur gestionnaire de clés (KMS). La clé est transférée à l'Agent de support (MA) qui configure le lecteur pour le cryptage et fournit la clé de cryptage au lecteur. Le lecteur crypte les données et les métadonnées qui sont écrites sur le support.

Lors d'une opération de copie ou de consolidation d'objet à partir d'une sauvegarde cryptée, les données sont décryptées par les lecteurs sources, transférées sur le réseau et cryptées par les lecteurs cibles.

Si un support source impliqué dans une session de copie automatique de supports contient des données cryptées et des données non cryptées, toutes les données écrites sur le support cible correspondant sont soit cryptées soit non cryptées, selon les paramètres en cours pour le cryptage sur lecteur.

La Figure 18 à la page 82 présente une interaction classique au cours d'une session de sauvegarde cryptée lorsque l'option de cryptage **AES 256 bits** et l'option **Cryptage sur lecteur** sont sélectionnées.



**Figure 18** Session de sauvegarde avec cryptage AES 256 bits et cryptage sur lecteur

## Restauration à partir de sauvegardes cryptées

Aucune préparation supplémentaire liée au cryptage n'est requise pour la restauration des sauvegardes cryptées, puisque Data Protector obtient automatiquement les clés de décryptage appropriées.

## Communications de contrôle cryptées

Les fonctions de communications de contrôle cryptées de Data Protector, qui permettent d'empêcher tout accès non autorisé, reposent sur le protocole cryptographique SSL (Secure Socket Layer) qui assure la sécurité des communications sur le réseau. SSL crypte les segments de connexions réseau et encapsule le protocole de communication Data Protector existant.

Les communications de contrôle dans une cellule Data Protector correspondent à tous les échanges entre les processus Data Protector, à l'exception du transfert de données de l'Agent de disque (et des intégrations) vers l'Agent de support, et vice versa. Data Protector utilise des algorithmes SSLv3 "export grade" avec des clés allant jusqu'à 512 bits pour le cryptage asymétrique et jusqu'à 64 bits pour le cryptage symétrique afin de crypter les communications de contrôle. Etant donné que le protocole SSL nécessite des certificats pour établir des communications cryptées, Data Protector fournit des certificats par défaut durant l'installation ou la mise à niveau.

## Fonctionnement des communications de contrôle cryptées dans Data Protector

Le Gestionnaire de cellule Data Protector contrôle les sessions de sauvegarde et de restauration, qui effectuent respectivement toutes les actions requises pour une sauvegarde ou une restauration. Le cryptage est activé client par client, ce qui signifie qu'il est soit activé soit désactivé pour toutes les communications de contrôle avec le client sélectionné.

Vous devez tout d'abord activer le cryptage sur un Gestionnaire de cellule, puis sur les clients de la cellule. Les clients qui ne sont pas supposés communiquer de façon confidentielle peuvent être placés dans une liste d'exceptions du Gestionnaire de cellule, ce qui leur permet de communiquer en mode non crypté. Avant d'accepter une connexion, les processus Data Protector vérifient la configuration locale (pour voir si le cryptage est activé, le certificat à utiliser, etc.). La connexion SSL est établie avec les paramètres de cryptage de la configuration locale.

Durant la session de sauvegarde, les processus Data Protector lisent les paramètres de cryptage dans la configuration locale. Le Gestionnaire de session de sauvegarde (BSM) établit une connexion SSL avec l'Agent de support et l'Agent de disque, et le protocole de communication Data Protector standard suit. L'Agent de disque établit ensuite une connexion de données avec l'Agent de support. La sauvegarde des données suit.

La [Figure 19](#) à la page 84 présente les interactions classiques au sein de la cellule Data Protector si les fonctions de communications de contrôle cryptées sont activées.

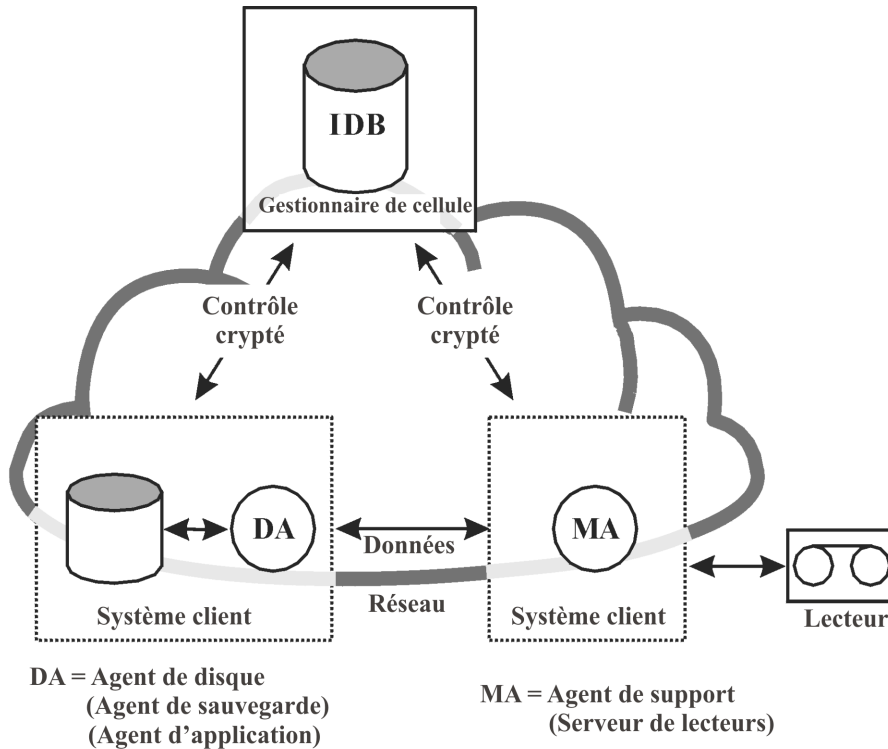


Figure 19 Communications de contrôle cryptées

## Cryptage des données et communications de contrôle cryptées

En combinant le cryptage des données avec les communications de contrôle cryptées, vous pouvez facilement renforcer la sécurité de votre système :

- Le cryptage sur logiciel (AES 256 bits) crypte les données avant leur transfert sur le réseau et leur enregistrement sur les supports.
- Le cryptage sur matériel (sur lecteur) de vos sauvegardes empêche les accès non autorisés à vos données durant le stockage sur le support et le transport.
- Les communications de contrôle cryptées sécurisent les échanges entre les clients de la cellule.

La [Figure 20](#) à la page 85 présente les interactions classiques au sein de la cellule Data Protector au cours d'une session de sauvegarde cryptée lorsque l'option de cryptage **AES 256 bits** et l'option **Cryptage sur lecteur** sont sélectionnées et les fonctions de communications de contrôle cryptées activées.

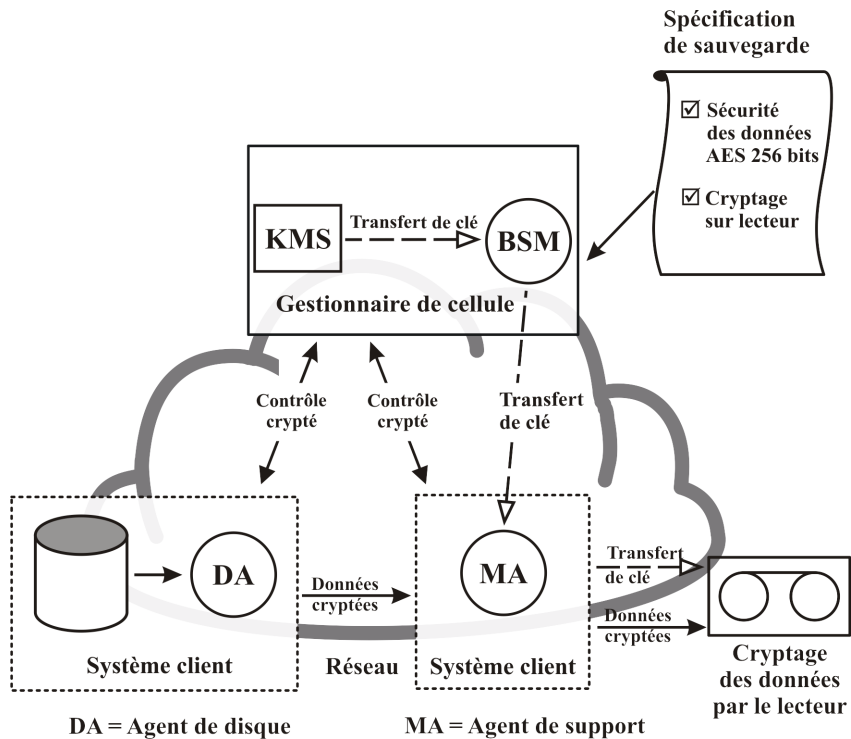


Figure 20 Communications de contrôle cryptées et cryptage des données

## Gestion de clusters

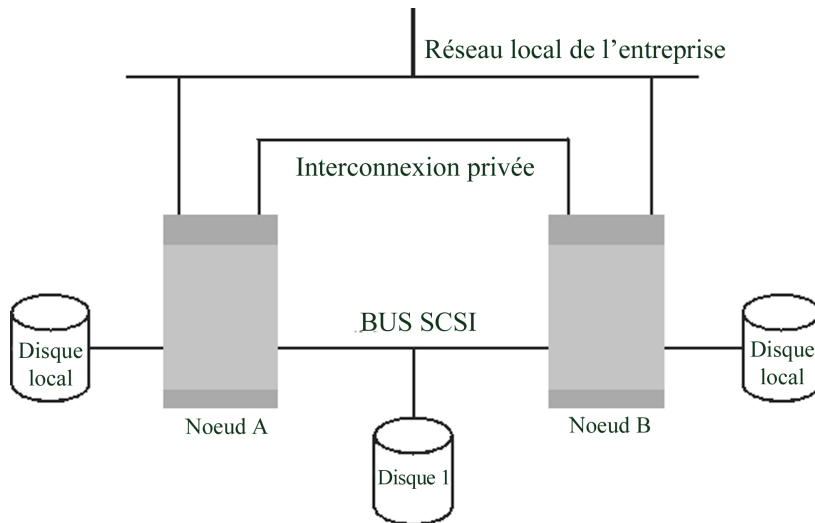
### Concepts rattachés aux clusters

#### Qu'est-ce qu'un cluster ?

Un **cluster** est un groupe de plusieurs ordinateurs qui apparaissent sur le réseau comme un système unique. Ce groupe d'ordinateurs est géré comme un système unique et destiné à :

- garantir une disponibilité des applications et ressources stratégiques aussi élevée que possible ;
- tolérer les pannes de composant ;
- prendre en charge l'ajout et le retrait de composants.

Sur le plan de la gestion des clusters, Data Protector est compatible avec Microsoft Cluster Server pour Windows Server, MC/Service Guard pour HP-UX, Veritas Cluster pour Solaris et Novell NetWare Cluster Services. Pour obtenir une liste des clusters pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.



**Figure 21 Structure d'un cluster type**

Composants :

- Nœuds de cluster (plusieurs)
- Disques locaux
- Disques partagés (entre les nœuds)

### Noeuds de cluster

**Les nœuds de cluster** sont les ordinateurs qui composent un cluster. Ils sont physiquement connectés à un ou plusieurs disques partagés.

### Disques partagés

Les **volumes de disques partagés** (MSCS, Novell NetWare Cluster Services) ou les **groupes de volumes partagés** (MC/SG, Veritas Cluster) contiennent des données d'application stratégiques, ainsi que des données de cluster spécifiques qui sont nécessaires au fonctionnement du cluster. Dans les clusters MSCS, un disque partagé est exclusivement actif sur un seul nœud de cluster à la fois.

## Réseau de cluster

Un réseau de cluster est un réseau privé qui relie tous les nœuds de cluster. Il transfère les données internes du cluster appelées **pulsation du cluster**. La pulsation est un paquet de données comportant un horodatage, distribué à tous les nœuds de cluster. Les nœuds de cluster, en comparant ces paquets, déterminent celui d'entre eux qui est toujours opérationnel, ce qui leur permet de déterminer l'appartenance du **package** (MC/SG, Veritas Cluster) ou **groupe** (MSCS).

### Qu'est-ce qu'un package ou groupe ?

Un package (MC/SG, Veritas Cluster) ou un groupe (MSCS) est un regroupement de ressources nécessaires à l'exécution d'une application **compatible cluster** spécifique. Toutes les applications compatibles cluster déclarent leurs propres ressources critiques. Les ressources suivantes doivent être définies dans chaque groupe ou package :

- Volumes de disques partagés (MSCS, Novell NetWare Cluster Services)
- Groupes de volumes partagés (MC/SG, Veritas Cluster)
- Noms IP réseau
- Adresses IP réseau
- Services d'application compatibles cluster

### Qu'est-ce qu'un serveur virtuel ?

Les volumes de disques et groupes de volumes représentent des disques physiques partagés. Le nom et l'adresse IP réseau composent les ressources permettant de définir le **serveur virtuel** d'une application compatible cluster. Son nom et son adresse IP sont mis en cache par le logiciel du cluster et mis en correspondance avec le nœud de cluster sur lequel le package ou le groupe s'exécute. Le groupe ou package pouvant basculer d'un nœud à l'autre, le serveur virtuel peut résider sur différentes machines à différentes périodes.

### Qu'est-ce qu'un basculement ?

Chaque package ou groupe dispose d'un nœud "favori", sur lequel il s'exécute habituellement. Ce nœud est appelé **nœud principal**. Un package ou un groupe peut être déplacé dans un autre nœud de cluster (l'un des **nœuds secondaires**). Le processus de transfert d'un package ou d'un groupe du nœud de cluster principal au nœud secondaire est appelé **basculement** ou passage. Le nœud secondaire accepte le package ou groupe en cas de panne du nœud principal. Un basculement peut se produire pour différentes raisons :

- En cas de pannes logicielles sur le nœud principal

- En cas de pannes matérielles sur le nœud principal
- Si l'administrateur effectue intentionnellement un transfert de propriété en raison d'une opération de maintenance sur le nœud principal

Dans un environnement de clusters, il peut y avoir plusieurs nœuds secondaires mais un seul nœud principal.

Un Gestionnaire de cellule Data Protector compatible cluster chargé d'exécuter la base de données IDB et de gérer les opérations de sauvegarde et de restauration présente des avantages remarquables par rapport à des versions non cluster.

### Haute disponibilité du Gestionnaire de cellule Data Protector

Toutes les opérations du Gestionnaire de cellule sont disponibles en permanence, les services Data Protector étant définis en tant que ressources de cluster dans le cluster et automatiquement redémarrés en cas de basculement.

### Redémarrage automatique des sauvegardes

Vous pouvez facilement configurer les spécifications de sauvegarde Data Protector qui définissent la procédure de sauvegarde afin qu'elles soient redémarrées en cas de basculement du Gestionnaire de cellule de Data Protector. Utilisez l'interface Data Protector pour définir les paramètres de redémarrage.

### Partage de charge en cas de basculement

Un utilitaire spécial de ligne de commande permet aux utilisateurs d'effectuer différentes opérations, et notamment l'abandon des sessions de sauvegarde au cas où des applications non Data Protector basculeraient. Le Gestionnaire de cellule Data Protector permet à l'administrateur de définir les opérations à exécuter dans ce type de situation. Si la sauvegarde a moins d'importance que l'application, Data Protector peut abandonner les sessions en cours. Si la sauvegarde est plus importante ou sur le point de se terminer, Data Protector peut poursuivre les sessions. Pour plus d'informations sur la procédure de définition de critères, recherchez l'entrée suivante dans l'index de l'aide en ligne : "cluster, gestion de sauvegardes".

## Support de clusters

Le support de clusters Data Protector signifie que :

- Le Gestionnaire de cellule Data Protector est installé dans un cluster. Un tel Gestionnaire de cellule tolère les pannes et peut *redémarrer* automatiquement des *opérations* dans la cellule après le basculement.



---

 **REMARQUE :**

Si le Gestionnaire de cellule est installé dans le cluster, ses ressources critiques de cluster doivent être configurées dans le même package ou groupe de clusters que l'application en cours de sauvegarde, afin de redémarrer automatiquement les *sessions de sauvegarde qui ont échoué* en raison d'un basculement. Dans le cas contraire, les sessions qui ont échoué doivent être redémarrées manuellement.

---

- Le client Data Protector est installé dans un cluster. Le Gestionnaire de cellules (s'il n'est pas installé dans le cluster) ne tolère pas les pannes dans ce cas. Les opérations de la cellule doivent donc être redémarrées manuellement.

Le comportement du Gestionnaire de cellule après le basculement peut être configuré en ce qui concerne la *session de sauvegarde* (ayant échoué en raison du basculement). Suite à l'échec d'une session, trois solutions sont possibles :

- le redémarrage complet
- le redémarrage des objets ayant échoué
- pas de redémarrage

Pour plus d'informations sur les options relatives au comportement de la session de sauvegarde en cas de basculement du Gestionnaire de cellule Data Protector, recherchez l'entrée suivante dans l'index de l'aide en ligne : "cluster, options de spécification de sauvegarde".

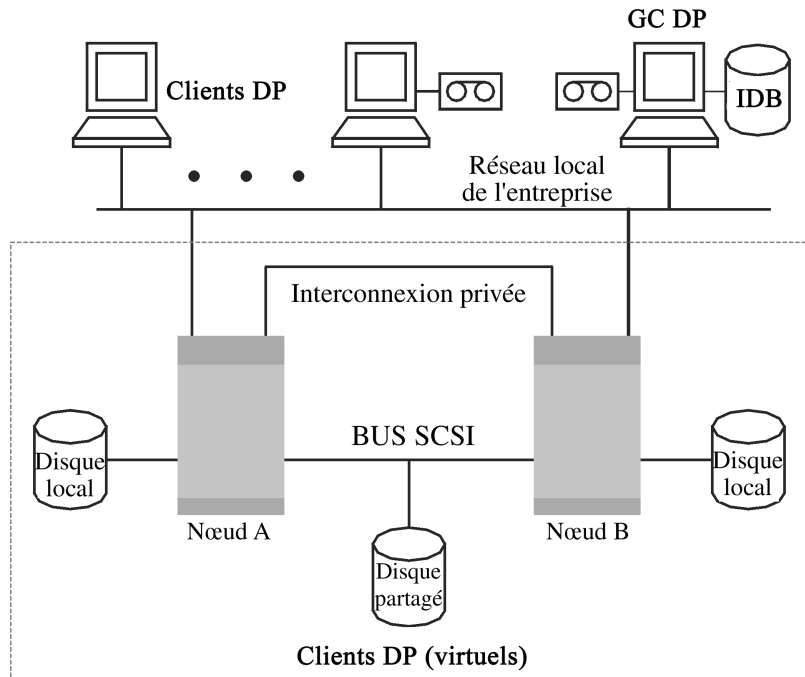
## Exemples d'environnements de clusters

Vous trouverez dans cette section trois exemples de configurations de cluster.

### Gestionnaire de cellule installé hors d'un cluster

L'environnement est le suivant :

- Le Gestionnaire de cellule est installé hors d'un cluster.
- Un périphérique de sauvegarde est connecté au Gestionnaire de cellule ou à l'un des clients (non regroupés en cluster).



**Figure 22 Gestionnaire de cellule installé hors d'un cluster**

Lorsque vous créez une spécification de sauvegarde, vous pouvez voir trois systèmes ou plus pouvant être sauvegardés dans le cluster.

- Nœud physique A
- Nœud physique B
- Serveur virtuel

### Sauvegarde du serveur virtuel

Si vous sélectionnez le serveur virtuel dans la spécification de sauvegarde, la session va alors sauvegarder le serveur/hôte virtuel actif sélectionné, indépendamment du nœud physique sur lequel le package ou groupe est en cours d'exécution.

Pour plus d'informations sur la procédure de ces options, recherchez l'entrée suivante dans l'index de l'aide en ligne : "cluster, options de spécification de sauvegarde".

Le tableau ci-dessous décrit le comportement prévu dans cette configuration.

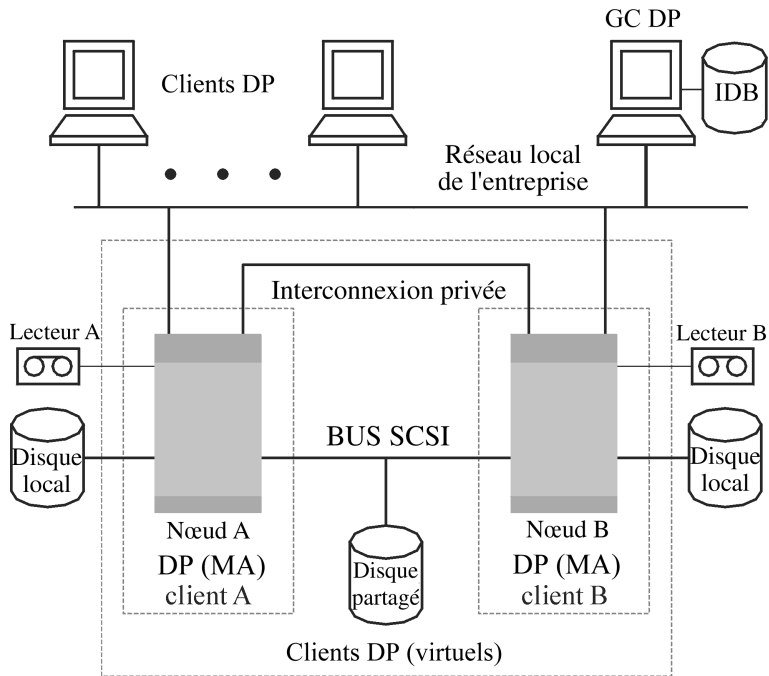
**Tableau 3 Comportement relatif à la sauvegarde**

Condition	Résultat
Basculement du nœud avant le démarrage de la sauvegarde	Sauvegarde réussie
Basculement du nœud pendant la sauvegarde	<b>Sauvegarde d'image disque/de système de fichiers</b> : échec de la session de sauvegarde. Les objets entièrement sauvegardés peuvent être utilisés pour effectuer les restaurations. En revanche, les objets ayant échoué (en cours d'exécution ou en attente) doivent être sauvegardés à nouveau en redémarrant manuellement la session.
	<b>Sauvegarde d'application</b> : échec de la session de sauvegarde. La session doit être redémarrée manuellement.

### Gestionnaire de cellule installé hors d'un cluster, périphériques connectés aux nœuds de cluster

L'environnement est le suivant :

- Le Gestionnaire de cellule est installé hors d'un cluster.
- Les périphériques de sauvegarde sont connectés aux nœuds du cluster.



**Figure 23 Gestionnaire de cellule installé hors d'un cluster, périphériques connectés aux nœuds de cluster**

Lorsque vous créez une spécification de sauvegarde, vous pouvez voir trois systèmes ou plus pouvant être sauvegardés dans le cluster.

- Nœud physique A
- Nœud physique B
- Serveur virtuel

### Sauvegarde du serveur virtuel

Si vous sélectionnez le serveur virtuel dans la spécification de sauvegarde, la session va alors sauvegarder le serveur/hôte virtuel actif sélectionné, indépendamment du nœud physique sur lequel le package ou groupe est en cours d'exécution.

---

 **REMARQUE :**

La différence avec l'exemple précédent réside dans le fait qu'un Agent de support Data Protector est installé sur chacun des nœuds du cluster. Vous devez en outre utiliser la fonctionnalité de partage de charge Data Protector. Incluez les deux périphériques dans la spécification de sauvegarde. Si vous définissez les valeurs de partage de charge à  $\text{min}=1$  et  $\text{max}=1$ , Data Protector n'utilisera que le premier périphérique disponible.

---

Le tableau ci-dessous décrit le comportement prévu dans cette configuration.

**Tableau 4 Comportement relatif à la sauvegarde**

Condition	Résultat
Basculement du nœud avant le démarrage de la sauvegarde	Sauvegarde réussie grâce au basculement automatique de périphérique (partage de charge)
Basculement du nœud pendant la sauvegarde	<b>Sauvegarde d'image disque/de système de fichiers :</b> échec de la session de sauvegarde. Les objets entièrement sauvegardés peuvent être utilisés pour effectuer les restaurations. En revanche, les objets ayant échoué (en cours d'exécution ou en attente) doivent être sauvegardés à nouveau en redémarrant manuellement la session.
	<b>Sauvegarde d'application :</b> échec de la session de sauvegarde. La session doit être redémarrée manuellement.

---

 **IMPORTANT :**

Si un basculement survient dans une telle configuration pendant une activité de sauvegarde, l'Agent de support risque d'abandonner la session de façon incorrecte, entraînant la corruption du support.

---

## Gestionnaire de cellule installé dans un cluster, périphériques connectés aux nœuds de cluster

L'environnement est le suivant :

- Le Gestionnaire de cellule est installé dans un cluster.  
En ce qui concerne les intégrations de l'application Data Protector, il existe deux façons de configurer Data Protector ainsi qu'une application dans une telle configuration :
  - Le Gestionnaire de cellule Data Protector est configuré pour s'exécuter (à la fois en exécution normale et lors du basculement) sur le même nœud que l'application. Les ressources critiques de cluster Data Protector sont définies dans le même package (MC/ServiceGuard) ou groupe (Microsoft Cluster Server) que les ressources critiques de cluster de l'application.

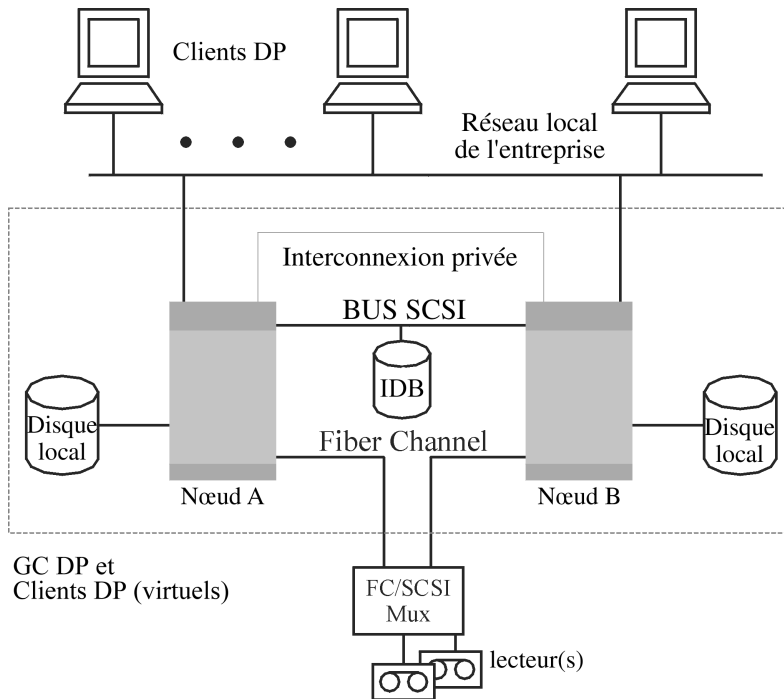
---

### ❗ IMPORTANT :

Seule cette configuration permet de définir une opération automatisée pour les sessions Data Protector abandonnées pendant le basculement.

---

- Le Gestionnaire de cellule Data Protector est configuré pour s'exécuter (à la fois en exécution normale et lors du basculement) sur des nœuds autres que celui de l'application. Les ressources critiques de cluster Data Protector sont définies dans un autre package (MC/ServiceGuard) ou groupe (Microsoft Cluster Server) que les ressources critiques de cluster de l'application.
- Le ou les périphériques de sauvegarde sont connectés au bus Fibre Channel partagé du cluster via un multiplexeur FC/SCSI.



**Figure 24 Gestionnaire de cellule installé dans un cluster, périphériques connectés aux nœuds de cluster**

Lorsque vous créez une spécification de sauvegarde, vous pouvez voir trois systèmes ou plus pouvant être sauvegardés dans le cluster.

- Nœud physique A
- Nœud physique B
- Serveur virtuel

### Sauvegarde du serveur virtuel

Si vous sélectionnez le serveur virtuel dans la spécification de sauvegarde, la session va alors sauvegarder le serveur/hôte virtuel actif sélectionné, indépendamment du nœud physique sur lequel le package ou groupe est en cours d'exécution.

---

 **REMARQUE :**

Les clusters ne prennent pas en charge les bus SCSI avec des bandes partagées. Pour que les Agents de support bénéficient eux aussi d'une grande disponibilité, la technologie Fibre Channel peut être utilisée comme une interface avec le périphérique. Le périphérique en tant que tel ne dispose pas d'une grande disponibilité dans cette configuration.

---

Dans cette configuration, vous pouvez accéder aux fonctions suivantes :

- Redémarrage automatique personnalisable des sauvegardes en cas de basculement du Gestionnaire de cellule.

Vous pouvez configurer les spécifications de sauvegarde Data Protector afin qu'elles soient redémarrées en cas de basculement du Gestionnaire de cellule. Utilisez l'interface Data Protector pour définir les paramètres de redémarrage.

- Contrôle des charges système au moment du basculement.

Un contrôle de pointe permet de définir le comportement de Data Protector en cas de basculement. La commande `omniclus` est prévue à cet effet. Le Gestionnaire de cellule permet à l'administrateur de définir les opérations à exécuter dans ce genre de situation.

- Si la sauvegarde a moins d'importance que l'application qui vient de basculer vers le système de sauvegarde, Data Protector peut abandonner les sessions en cours.
- Si elle a plus d'importance ou qu'elle est sur le point d'être effectuée, Data Protector poursuit les sessions.

Le tableau ci-dessous décrit le comportement prévu dans cette configuration.

**Tableau 5 Comportement relatif à la sauvegarde**

Condition	Résultat
Basculement avant le début d'une sauvegarde	Sauvegarde réussie



Condition	Résultat	
<p>Basculement de l'application et du Gestionnaire de cellule pendant la sauvegarde (le Gestionnaire de cellule s'exécute sur le même nœud que l'application).</p>	<p><b>Sauvegarde d'image disque/de système de fichiers</b> : échec de la session de sauvegarde. Les objets entièrement sauvegardés peuvent être utilisés pour effectuer des restaurations. Par contre, les objets dont la sauvegarde a échoué (en cours d'exécution ou en attente) doivent être sauvegardés à nouveau en redémarrant manuellement la session.</p>	<p><b>IMPORTANT</b></p> <p>Pour redémarrer la session, il est important de sélectionner l'option appropriée dans Data Protector. Pour plus d'informations sur la définition de toutes les actions Data Protector possibles en cas de basculement du Gestionnaire de cellule, recherchez l'entrée suivante dans l'index de l'aide en ligne : "cluster, gestion de sauvegardes".</p>
	<p><b>Sauvegarde d'application</b> : échec de la session de sauvegarde. Cette session est redémarrée automatiquement.</p>	
<p>Basculement de l'application pendant la sauvegarde sans basculement du Gestionnaire de cellule (ce dernier s'exécute sur un nœud autre que celui de l'application).</p>	<p><b>Sauvegarde d'image disque/de système de fichiers</b> : la session de sauvegarde échoue lors du basculement du nœud sur lequel le système de fichiers est installé. Les objets entièrement sauvegardés peuvent être utilisés pour effectuer les restaurations. En revanche, les objets ayant échoué (en cours d'exécution ou en attente) doivent être sauvegardés à nouveau en redémarrant manuellement la session.</p>	
	<p><b>Sauvegarde d'application</b> : échec de la session de sauvegarde. La session doit être redémarrée manuellement.</p>	

❗ **IMPORTANT :**

Si un basculement survient dans une telle configuration pendant une activité de sauvegarde, l'Agent de support risque d'abandonner la session de façon incorrecte, entraînant la corruption du support.

En outre, le Gestionnaire de cellule/client du cluster Data Protector peut être intégré à l'environnement EMC Symmetrix ou HP StorageWorks Disk Array XP, ce qui a pour effet d'augmenter considérablement la disponibilité de l'environnement de sauvegarde. Pour plus d'informations, reportez-vous au *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

## Sauvegardes complètes et incrémentales

Data Protector propose deux types de sauvegarde de système de fichiers de base : la sauvegarde complète et la sauvegarde incrémentale.

Une sauvegarde complète consiste à enregistrer l'ensemble des fichiers sélectionnés pour la sauvegarde dans un système de fichiers. Une sauvegarde incrémentale consiste à n'enregistrer que les fichiers modifiés depuis la dernière sauvegarde complète ou incrémentale. Cette section comporte des conseils pour choisir un type de sauvegarde et décrit l'incidence que peut avoir votre choix sur votre stratégie de sauvegarde.

**Tableau 6 Comparaison entre la sauvegarde complète et la sauvegarde incrémentale**

	<b>Sauvegarde complète</b>	<b>Sauvegarde incrémentale</b>
<b>Ressources</b>	Prend plus de temps que la sauvegarde incrémentale et requiert davantage de supports.	Ne sauvegarde que ce qui a été modifié depuis la dernière sauvegarde, ce qui permet de gagner du temps et d'économiser de l'espace sur les supports.
<b>Gestion de périphériques</b>	Si vous utilisez un périphérique autonome comportant un seul lecteur, vous devrez remplacer le support manuellement si l'intégralité du contenu de la sauvegarde ne tient pas sur un seul support.	Il est moins probable que la sauvegarde requiert des supports supplémentaires.
<b>Restauration</b>	Restauration simple et rapide.	Une restauration prend plus de temps en raison du nombre de supports nécessaires.
<b>Impact IDB</b>	Occupe plus d'espace dans la base de données IDB.	Occupe moins d'espace dans la base de données IDB.

Data Protector vous permet également d'effectuer des sauvegardes incrémentales d'applications de base de données en ligne. Celles-ci peuvent varier d'une application à l'autre. Pour Sybase, par exemple, ce type de sauvegarde est appelé "sauvegarde de transactions" et consiste à sauvegarder les journaux de transactions modifiés depuis la sauvegarde précédente.

Notez que le concept de sauvegarde incrémentale n'est pas lié au concept de niveau de journalisation qui, quant à lui, permet de définir la quantité d'informations écrites dans la base de données IDB.



---

## REMARQUE :

Un certain nombre de types de sauvegardes supplémentaires (Split Mirror, Snapshot et Data Mover) sont disponibles grâce aux intégrations d'applications Data Protector. Pour plus d'informations, reportez-vous au *Guide d'intégration HP Data Protector* correspondant.

---

## Sauvegardes complètes

Les sauvegardes complètes sont des sauvegardes au cours desquelles tous les objets sélectionnés sont sauvegardés, même s'ils n'ont pas été modifiés depuis la sauvegarde précédente.

## Sauvegarde synthétique

La sauvegarde synthétique est une solution de sauvegarde avancée qui évite d'avoir à lancer régulièrement des sauvegardes complètes. Cette solution permet de réaliser des sauvegardes incrémentales aussitôt fusionnées avec la sauvegarde complète pour obtenir une nouvelle sauvegarde complète synthétique. Pour plus de détails, reportez-vous au [Chapitre 10](#) à la page 275.

## Sauvegardes incrémentales

Les sauvegardes incrémentales permettent de sauvegarder les modifications par rapport à une sauvegarde (complète ou incrémentale) précédente toujours protégée. Pour procéder à la sauvegarde incrémentale d'un objet, une sauvegarde complète de l'objet en question (avec un nom de client, un point de montage et une description identiques) doit avoir été effectuée au préalable.

Les sauvegardes incrémentales dépendent de la dernière sauvegarde complète effectuée. Si vous définissez une sauvegarde incrémentale sans avoir effectué une sauvegarde complète protégée, le système procède à une sauvegarde complète.

## Sauvegarde incrémentale classique

Avant d'effectuer une sauvegarde incrémentale d'un objet sauvegarde spécifique, Data Protector compare les arborescences de l'objet sauvegarde à celles de la chaîne de restauration valide de l'objet en question. Si les arborescences ne concordent pas (par exemple, un répertoire supplémentaire de l'objet sauvegarde a été sélectionné pour la sauvegarde depuis la dernière sauvegarde ou il existe plusieurs

spécifications de sauvegarde avec le même objet sauvegarde et des arborescences différentes), une sauvegarde complète est exécutée automatiquement. De cette manière, tous les fichiers modifiés depuis la dernière sauvegarde pertinente sont sauvegardés.

Dans la sauvegarde incrémentale classique, c'est l'heure de modification du fichier qui permet de déterminer si ce dernier a été modifié ou non depuis la dernière sauvegarde. Cependant, même si le fichier a été renommé, déplacé ou si certains de ses attributs ont été modifiés, l'heure de modification ne change pas et le fichier n'est donc pas sauvegardé lors de la sauvegarde incrémentale classique. De tels fichiers ne pourront être sauvegardés qu'à la sauvegarde complète suivante.

## Sauvegarde incrémentale avancée

Une sauvegarde incrémentale avancée est capable de détecter et de sauvegarder les fichiers renommés et déplacés, ainsi que ceux dont les attributs ont été modifiés.

Ce type de sauvegarde permet également d'éviter les sauvegardes complètes inutiles d'un objet sauvegarde dans son intégralité lorsque certaines des arborescences sélectionnées pour la sauvegarde changent. Par exemple, si un répertoire supplémentaire a été sélectionné pour la sauvegarde depuis la dernière sauvegarde, une sauvegarde complète de ce répertoire (arborescence) est exécutée, tandis que les éléments restants font l'objet d'une sauvegarde incrémentale.

L'utilisation de la sauvegarde incrémentale avancée est un prérequis à la sauvegarde synthétique.

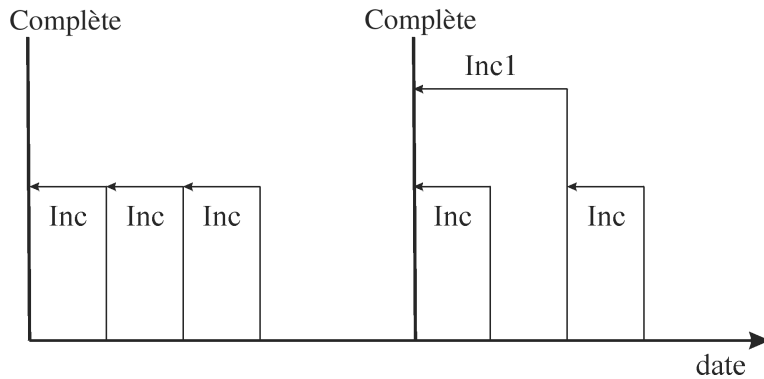
## Sauvegarde incrémentale au moyen du module fournisseur d'informations sur les modifications

Vous pouvez effectuer des sauvegardes incrémentales avancées ou des sauvegardes incrémentales standard en utilisant le module fournisseur d'informations sur les modifications Windows NTFS. Ce module interroge le journal des modifications Windows pour obtenir la liste des fichiers modifiés au lieu d'effectuer une recherche fastidieuse dans l'arborescence des fichiers. Comme le journal des modifications détecte et enregistre toutes les modifications apportées aux fichiers et aux répertoires dans un volume NTFS, Data Protector peut l'utiliser comme mécanisme de suivi pour générer la liste des fichiers modifiés depuis la dernière sauvegarde complète. La sauvegarde incrémentale est ainsi beaucoup plus rapide, en particulier dans des environnements contenant des millions de fichiers dont seuls quelques-uns ont été modifiés, et permet d'éliminer des sauvegardes complètes inutiles.

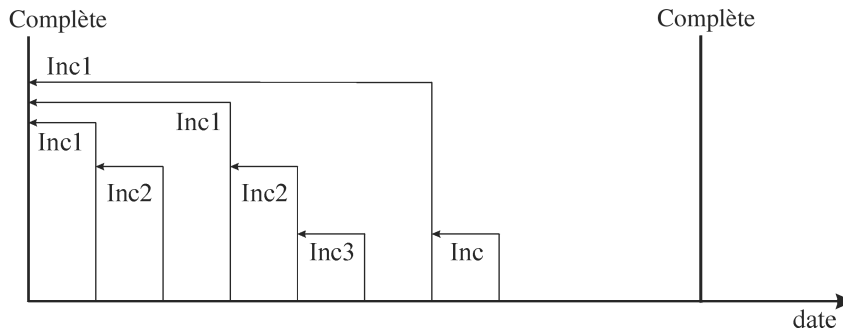
## Types de sauvegardes incrémentales

Dans Data Protector, différents types de sauvegardes incrémentales sont disponibles :

- Incr. Une sauvegarde incrémentale simple (voir [Figure 25](#) à la page 102) est basée sur la dernière sauvegarde encore protégée, qui peut être une sauvegarde complète ou incrémentale.
  
- Incr1-9 Une **sauvegarde incrémentale par niveau** (voir [Figure 26](#) à la page 102) dépend de la dernière sauvegarde en date du niveau immédiatement inférieur, dont les données sont toujours protégées. Par exemple, lors d'une sauvegarde Incr1, toutes les modifications effectuées depuis la dernière sauvegarde complète seront sauvegardées, alors que lors d'une sauvegarde Incr5, seules les modifications effectuées depuis la dernière sauvegarde Incr4 seront sauvegardées. Une sauvegarde Incr1-9 ne fait *jamais* référence à une sauvegarde Incr existante.



**Figure 25 Sauvegardes incrémentales**



**Figure 26 Sauvegardes incrémentales par niveau**

Le [Tableau 7](#) à la page 102 décrit les références relatives pour l'exécution de sauvegardes basées sur différents types de sauvegardes. Pour une lecture détaillée, voir le texte explicatif au-dessous du tableau.

**Tableau 7 Références relatives des différentes sauvegardes**

1	Complète	<---	Incr. 1				
2	Complète	<---	<---	<---	Incr. 2		
3	Complète	<---	Incr. 1	<---	Incr. 2		
4	Complète	<---	Incr.				
5	Complète	<---	Incr. 1	<---	Incr.		
6	Complète	<---	Incr. 1	<---	Incr. 2	<---	Incr.
7	Complète	<---	Incr. 1	<---	Incr.	<---	Incr.

8	Complète	<---	Incr. 1	<---	Incr. 3		
9	Complète	<---	Incr. 1	<---	Incr. 2	<---	Incr. 3
10	Complète	<---	<---	<---	Incr. 2	<---	Incr. 3
11	Complète	<---	<---	<---	<---	<---	Incr. 3

### Comment lire le Tableau 7 à la page 102

- Les lignes du [Tableau 7](#) à la page 102 sont indépendantes les unes des autres et décrivent des situations différentes.
- L'âge des sauvegardes augmente de la droite vers la gauche, c'est-à-dire que la sauvegarde qui se trouve le plus à gauche est la plus ancienne alors que celle qui se trouve le plus à droite est la plus récente.
- Complète et Incr. X sont des objets statiques protégés du même propriétaire. Un objet Incr. X non protégé peut être utilisé pour la restauration, mais ne peut en aucun cas servir de référence pour des sauvegardes ultérieures.

### Exemples

- A la deuxième ligne, vous pouvez voir une sauvegarde Complète statique protégée et une sauvegarde Incr. 2 en cours d'exécution. Il n'y a pas de Incr. 1, donc la sauvegarde est exécutée comme une Incr. 1.
- A la 5ème ligne, vous trouvez une sauvegarde Complète, une Incr. 1 et une autre sauvegarde incrémentale en cours d'exécution. Pour la sauvegarde en cours, Data Protector se réfère à la sauvegarde précédente, c'est-à-dire Incr. 1.
- A la 8ème ligne, Incr. 3 est exécutée comme une Incr. 2 et à la 11ème ligne, Incr. 3 est exécutée comme une Incr. 1.

## Observations relatives à la restauration

Pour restaurer les dernières données sauvegardées, vous avez besoin des supports sur lesquels sont stockées la sauvegarde complète la plus récente et les sauvegardes incrémentales qui ont suivi. Par conséquent, plus le nombre de sauvegardes incrémentales effectuées est important, plus vous aurez de supports à gérer. Cela peut présenter un inconvénient si vous utilisez des périphériques autonomes, et la restauration peut durer assez longtemps.

L'utilisation de sauvegardes incrémentales simples et par niveau (voir [Figure 27](#) à la page 105) requiert l'accès aux cinq **jeux de supports** les plus récents, jusqu'à la sauvegarde complète incluse. L'espace nécessaire sur les supports est moins important

dans ce cas, mais la restauration quelque peu complexe. La série de jeux de supports requis est également appelée **chaîne de restauration**.

---

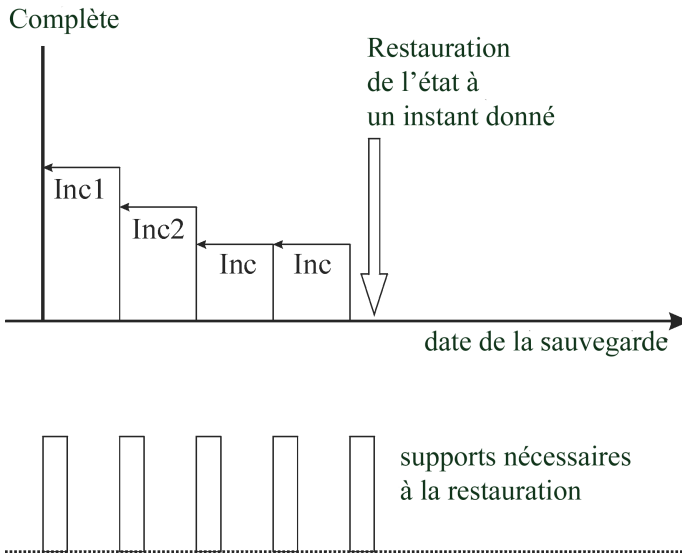
 **CONSEIL :**

Utilisez l'option **Ajout possible aux incrémentales uniquement** de Data Protector pour stocker les données provenant de sauvegardes complètes et incrémentales (avec la même spécification de sauvegarde) sur un même jeu de sauvegarde.

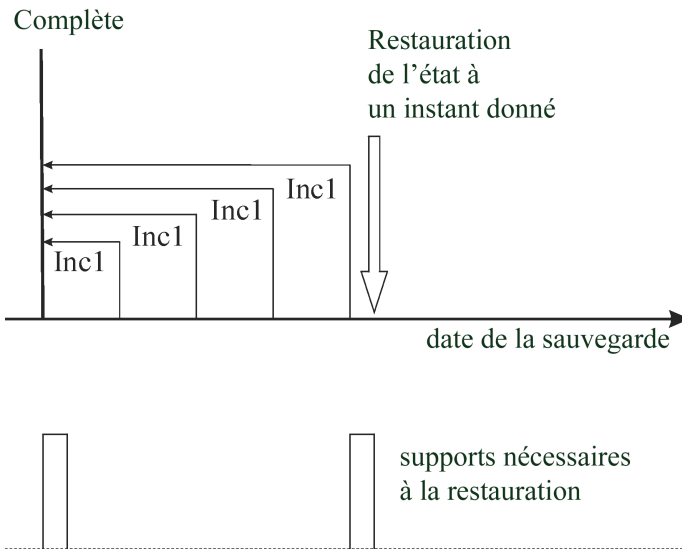
---

Une autre utilisation courante du concept de sauvegarde incrémentale est illustrée à la [Figure 28](#) à la page 105. Dans ce cas, l'espace nécessaire sur les supports est légèrement plus important. Vous n'avez besoin d'accéder à deux jeux de supports que pour procéder à la restauration des données à un instant donné. Notez qu'il n'existe aucune dépendance avec un jeu de supports Incr1 précédent éventuel pour cette restauration, sauf si vous déplacez l'instant donné pour la restauration en question.





**Figure 27 Supports nécessaires à la restauration à partir de sauvegardes incrémentales simples et par niveau**



**Figure 28 Supports nécessaires à la restauration à partir de sauvegardes incrémentales par niveau**

Notez que vous devez définir la stratégie de protection des données appropriée pour obtenir toutes les sauvegardes complètes et incrémentales requises pour la

restauration. Si la protection des données n'est pas correctement définie, il est possible que la chaîne de sauvegarde soit rompue. Pour plus de détails, reportez-vous à l'[Annexe B](#) à la page 355.

## Conservation des données sauvegardées et des informations sur les données

Dans Data Protector, vous pouvez définir la durée pendant laquelle doivent être conservées les données sauvegardées sur le support lui-même (protection des données) et les informations sur les données sauvegardées dans la base de données IDB (protection de catalogue), ainsi que le niveau de ces informations (niveau de journalisation).

Vous pouvez définir la protection des données sauvegardées indépendamment de celle des informations de sauvegarde dans la base de données IDB. Lorsque vous copiez un support, vous pouvez définir pour les copies une période de protection différente de celle de l'original.

### Base de données interne de Data Protector

Les performances de restauration dépendent en partie du temps nécessaire au système pour trouver les supports requis pour une restauration. Par défaut, ces informations sont stockées dans la base de données interne IDB afin d'optimiser les performances de restauration et de permettre à l'utilisateur de parcourir les fichiers et répertoires à restaurer. Toutefois, stocker tous les noms de fichier de toutes les sauvegardes dans l'IDB et les conserver pendant longtemps risque de faire croître la taille de celle-ci dans des proportions qui la rendront impossible à gérer.

En permettant de spécifier la protection de catalogue indépendamment de la protection des données, Data Protector vous permet de trouver un compromis entre la croissance de l'IDB et la commodité de restauration des données. Vous pouvez, par exemple, mettre en œuvre une stratégie pour une restauration facile et rapide des données dans les quatre semaines suivant la sauvegarde, en définissant la protection de catalogue à quatre semaines. Passé ce délai, vous aurez toujours la possibilité d'effectuer des restaurations, moins facilement toutefois, et ce jusqu'à ce que la protection des données expire, à savoir au bout d'un an environ. En procédant ainsi, vous réduirez considérablement la taille de l'IDB.

## Protection des données

### Qu'est-ce que la protection des données ?

Data Protector vous permet de spécifier pendant combien de temps les données stockées sur les supports doivent être protégées contre tout écrasement par Data Protector. Cette protection peut être définie en dates absolues ou relatives.

Différentes parties de Data Protector vous permettent de définir la protection des données. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "protection des données".

Si vous ne changez pas l'option de sauvegarde **Protection des données** lors de la configuration d'une sauvegarde, les données sont protégées définitivement. Notez que si vous ne modifiez pas cette protection, le nombre de supports nécessaires pour les sauvegardes augmentera constamment.

## Protection de catalogue

### Qu'est-ce que la protection de catalogue ?

Data Protector enregistre des informations sur les données sauvegardées dans l'IDB. Ces informations étant écrites dans la base de données lors de chaque sauvegarde, la taille de l'IDB augmente avec le nombre et la taille des sauvegardes effectuées. La protection de catalogue indique à Data Protector la durée pendant laquelle les informations sur les données sauvegardées sont accessibles aux utilisateurs par exploration durant la restauration. Lorsque la protection de catalogue arrive à expiration, Data Protector écrase ces informations dans l'IDB (et non sur le support) en les remplaçant par d'autres lors d'une sauvegarde ultérieure.

Cette protection peut être définie en dates absolues ou relatives.

Si vous ne changez pas l'option de sauvegarde **Protection de catalogue** lors de la configuration de votre sauvegarde, les informations sur les données sauvegardées seront protégées aussi longtemps que les données correspondantes. Notez que si vous ne modifiez pas ce paramètre, la taille de l'IDB augmentera constamment en fonction des informations ajoutées avec chaque sauvegarde.

Pour plus d'informations sur la manière dont la protection de catalogue influe sur les performances et la croissance de l'IDB, reportez-vous à la section "[Protection de catalogue comme paramètre clé réglable de l'IDB](#)" à la page 223.

Le modèle de protection utilisé par Data Protector peut être mis en correspondance avec le concept de génération de sauvegarde présenté à l'[Annexe B](#) à la page 355.

## Niveau de journalisation

### Qu'est-ce que le niveau de journalisation ?

Le niveau de journalisation indique la quantité de détails sur les fichiers et répertoires, écrits dans l'IDB pendant la sauvegarde. Vous pouvez toujours restaurer vos données, sans tenir compte du niveau de journalisation utilisé pendant la sauvegarde.

Data Protector propose quatre niveaux de journalisation permettant de contrôler la quantité de détails sur les fichiers et répertoires écrits dans l'IDB. Pour plus de détails, reportez-vous à la section "[Niveau de journalisation comme paramètre clé réglable de l'IDB](#)" à la page 221.

## Exploration des fichiers à restaurer

L'IDB conserve des informations sur les données sauvegardées. Ces informations vous permettent de parcourir et de sélectionner des fichiers, et de démarrer leur restauration à l'aide de l'interface Data Protector. Vous pouvez également restaurer des données sans ces informations, à condition que les supports sur lesquels elles sont stockées soient toujours disponibles, mais vous devez pour cela savoir quel support utiliser et quelles données restaurer, par exemple le nom exact du fichier qui vous intéresse.

L'IDB contient également des informations concernant la durée pendant laquelle les données stockées sur le support ne seront pas écrasées.

Les stratégies adoptées en matière de protection des données, de protection de catalogue et de niveau de journalisation ont une incidence sur la disponibilité des données et sur le temps nécessaire pour y accéder pendant la restauration.

## Activation de l'exploration des fichiers et de la restauration rapide

Pour pouvoir restaurer des fichiers rapidement, les informations sur les données sauvegardées doivent exister dans le catalogue tout comme les données protégées sur le support. Les informations du catalogue vous permettent de parcourir et de sélectionner des fichiers, et de démarrer leur restauration à l'aide de l'interface utilisateur de Data Protector ; elles permettent également à Data Protector de localiser rapidement les données sur les supports de sauvegarde.

## Activation de la restauration des fichiers, sans l'exploration

Lorsque la protection de catalogue arrive à expiration et que les données sont toujours protégées, vous ne pouvez plus parcourir les fichiers dans l'interface de Data Protector ; cependant, la restauration des données reste possible si vous connaissez le nom du fichier à restaurer et le support sur lequel il est stocké. La restauration est moins rapide, car Data Protector ignore où se trouvent les données sur le support. Vous pouvez également réimporter le contenu du support dans la base de données IDB, ce qui revient à rétablir les informations sur les données sauvegardées dans le catalogue, puis lancer la restauration.

## Ecrasement des fichiers sauvegardés par de nouvelles données

Une fois que la protection des données est arrivée à expiration, les données stockées sur les supports sont écrasées lors d'une sauvegarde ultérieure. Tant que les données n'ont pas été écrasées, vous pouvez les restaurer à partir du support.

---

### CONSEIL :

Définissez la protection des données sur la durée pendant laquelle les données doivent être conservées, par exemple, un an.

Définissez, pour la protection de catalogue, la durée pendant laquelle vous souhaitez pouvoir parcourir, sélectionner et restaurer des fichiers rapidement à l'aide de l'interface utilisateur de Data Protector.

---

## Exportation de supports d'une cellule

L'exportation de supports d'une cellule Data Protector revient à supprimer de la base de données IDB toutes les informations sur les données sauvegardées sur ce support et les supports eux-mêmes. Vous ne pouvez pas parcourir, sélectionner ou restaurer des fichiers provenant d'un support exporté avec l'interface de Data Protector. Vous devez pour cela relire (ou ajouter) le support dans la cellule Data Protector. Cette fonction est nécessaire pour déplacer le support vers une autre cellule.

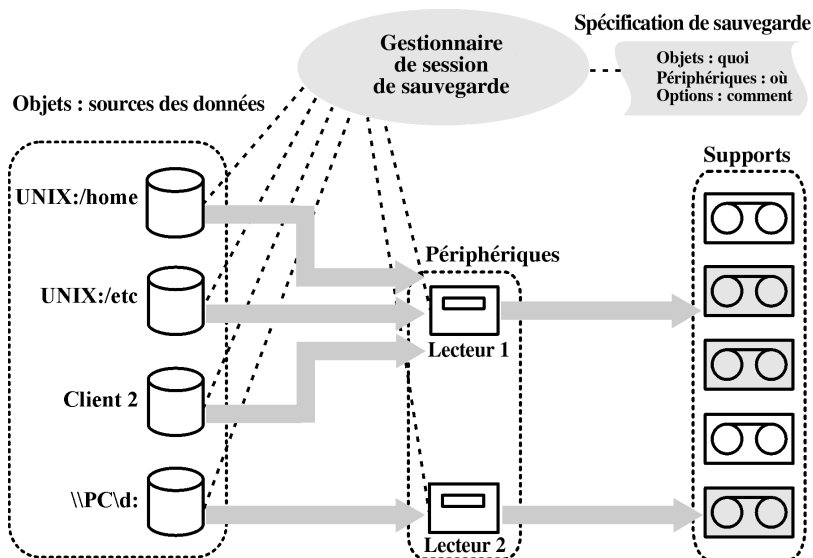
Au cours de l'exportation de supports, les informations de cryptage relatives aux supports sont également exportées dans un fichier .csv dans le répertoire d'exportation. Ce fichier est nécessaire pour la restauration de sauvegardes cryptées après la réimportation ou l'importation dans une autre cellule.

# Sauvegarde de données

La sauvegarde de données comporte l'une ou plusieurs des étapes suivantes :

- Sélection des données à sauvegarder et du système client source
- Sélection du système de destination sur lequel les données seront sauvegardées
- Sélection afin d'écrire des données identiques sur des jeux de supports supplémentaires - écriture en miroir
- Sélection des options de sauvegarde
- Planification d'une opération de sauvegarde automatisée

Vous pouvez spécifier tous ces éléments lors de la création d'une spécification de sauvegarde.



**Figure 29** Session de sauvegarde

À l'heure spécifiée, Data Protector démarre une session de sauvegarde sur la base d'une spécification de sauvegarde. La source de données est définie sous forme d'une liste d'objets (comme un système de fichiers sous UNIX ou des lecteurs de disque sous Windows) et les destinations sont des périphériques (à bandes par exemple) spécifiés. Au cours de la session de sauvegarde, Data Protector lit le contenu des objets, transfère les données via le réseau et les écrit sur les supports placés dans les périphériques. Le nom des périphériques à utiliser figure dans la spécification de sauvegarde. Un pool de supports peut également y être spécifié. Dans le cas contraire,

le pool par défaut est utilisé. Une spécification de sauvegarde peut être une simple définition de la sauvegarde d'un disque sur un lecteur DDS autonome, ou une définition complexe de la sauvegarde de 40 serveurs volumineux sur une bibliothèque à bande Silo comportant huit lecteurs.

## Création d'une spécification de sauvegarde

### Qu'est-ce qu'une spécification de sauvegarde ?

Une spécification de sauvegarde vous permet de regrouper les objets à sauvegarder en un groupe possédant des caractéristiques communes, comme la planification définie, les périphériques utilisés, le type de sauvegarde effectuée et les options sélectionnées pour la session sauvegarde.

### Comment créer une spécification de sauvegarde ?

Pour configurer une spécification de sauvegarde, utilisez l'interface de Data Protector. Vous devez pour cela savoir quelles données sauvegarder, combien de miroirs vous souhaitez créer, quels supports et quels périphériques utiliser pour la sauvegarde et, le cas échéant, définir certains comportements spécifiques pour la sauvegarde. Data Protector propose un comportement de sauvegarde par défaut adapté à la plupart des cas que vous pouvez rencontrer. Vous pouvez personnaliser le comportement de sauvegarde à l'aide des options de sauvegarde de Data Protector.

Data Protector vous permet de sauvegarder un client avec l'ensemble des disques qui y sont connectés, en détectant ces derniers au moment de la sauvegarde. Reportez-vous à la section "[Sauvegarde en mode détection de disques](#)" à la page 244.

## Sélection d'objets sauvegarde

### Qu'est-ce qu'un objet sauvegarde ?

Data Protector utilise le terme **objet sauvegarde** pour désigner une unité de sauvegarde qui contient tous les éléments sélectionnés pour la sauvegarde à partir d'un volume de disque (disque logique ou point de montage). Les éléments sélectionnés 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 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 : point d'accès dans une structure de répertoires (lecteur sous Windows et point de montage sous UNIX) sur le client contenant l'objet sauvegarde.
- Description : définit exclusivement les objets sauvegarde avec un nom de client et un point de montage identiques.
- Type : type d'objet sauvegarde, par exemple, un système de fichier ou Oracle.

Le mode de définition d'un objet sauvegarde est primordial pour comprendre la manière dont les sauvegardes incrémentales sont effectuées. Par exemple, si la description d'un objet sauvegarde change, l'objet en question est considéré comme un nouvel objet sauvegarde ; par conséquent, une sauvegarde complète doit automatiquement être effectuée à la place de la sauvegarde incrémentale.

### Exemples d'options de sauvegarde

Vous pouvez personnaliser le comportement relatif à la sauvegarde de chaque objet, en particulier en définissant des options de sauvegarde pour cet objet. Voici quelques exemples d'options de sauvegarde que vous pouvez spécifier :

- Niveau de journalisation des informations destinées à la base de données IDB  
Data Protector propose quatre niveaux de journalisation permettant de contrôler la quantité de détails concernant les fichiers et répertoires stockés dans la base de données IDB :
  - Journaliser tout
  - Fichiers journaux
  - Journaliser répertoires
  - Pas de journalisation

Notez que lorsque vous changez le niveau des informations stockées, les possibilités d'exploration des fichiers via l'interface Data Protector durant la restauration s'en trouvent affectées. Pour plus de détails sur les niveaux de journalisation, reportez-vous à la section "[Niveau de journalisation comme paramètre clé réglable de l'IDB](#)" à la page 221.
- Partage de charge automatique  
Allocation de périphérique dynamique à partir d'une liste donnée. Pour plus de détails, reportez-vous à la section "[Fonctionnement du partage de charge](#)" à la page 173.  
Cette option permet à Data Protector de déterminer de manière dynamique les périphériques sur lesquels les objets (disques) doivent être sauvegardés.
- Scripts pré-exécution et post-exécution



Traitement destiné à préparer un client à une sauvegarde cohérente. Pour plus de détails, reportez-vous à la section “[Commandes pré-exécution et post-exécution](#)” à la page 242.

- Sécurité des données

Niveau de sécurité à appliquer aux données.

Data Protector fournit trois niveaux de sécurité pour les données sauvegardées :

- Aucune
- AES 256 bits
- Encoder

Pour plus d'informations sur le cryptage, reportez-vous à la section “[Cryptage des données](#)” à la page 79.

Vous pouvez également spécifier les répertoires à exclure d'une sauvegarde ou ne sauvegarder que certains répertoires, ou encore sauvegarder les disques au fur et à mesure qu'ils sont ajoutés. Votre sauvegarde est donc entièrement configurable et dynamique.

## Sessions de sauvegarde

### Qu'est-ce qu'une session de sauvegarde ?

Une session de sauvegarde est un processus consistant à sauvegarder les données d'un système client sur des supports. Ce processus s'exécute toujours sur le système du Gestionnaire de cellule. Une session de sauvegarde est basée sur une spécification de sauvegarde et démarre lorsqu'une sauvegarde est exécutée.

Au cours d'une session de sauvegarde, Data Protector sauvegarde les données à l'aide du comportement par défaut ou de celui que vous avez défini.

Reportez-vous au [Chapitre 7](#) à la page 237 pour obtenir des informations détaillées sur les sessions de sauvegarde et sur la manière de les contrôler.

## Miroirs d'objet

### Qu'est-ce qu'un miroir d'objet ?

Le miroir d'objet est une copie supplémentaire d'un objet sauvegarde qui est créée pendant une session de sauvegarde. Lors de la création d'une spécification de sauvegarde, vous pouvez choisir de créer une ou plusieurs copies supplémentaires (miroirs) d'objets spécifiques. L'utilisation de la mise en miroir d'objet améliore la tolérance aux pannes des sauvegardes et permet d'effectuer une mise au coffre sur

plusieurs sites. Toutefois, la mise en miroir d'objet pendant une session de sauvegarde augmente le temps nécessaire à la sauvegarde.

Pour plus de détails, reportez-vous à la section "[Mise en miroir d'objets](#)" à la page 130.

## Jeux de supports

### Qu'est-ce qu'un jeu de supports ?

Le résultat d'une session de sauvegarde est un ensemble de données stockées sur un support ou un jeu de supports. Chaque session de sauvegarde produit un ou plusieurs jeux de supports, selon que la sauvegarde s'accompagne ou non de la mise en miroir d'objet. Selon l'utilisation qui est faite du pool, plusieurs sessions peuvent partager les mêmes supports. Lorsque vous restaurez des données, vous devez savoir à partir de quels supports effectuer la restauration. Data Protector conserve ces informations dans la base de données catalogue.

## Types de sauvegarde et sauvegardes planifiées

Une stratégie de planification permet de déterminer à quel moment démarrent les sauvegardes et de définir le type de sauvegarde effectuée (complète ou incrémentale). Prenez en compte les différences entre sauvegardes complètes et incrémentales. Reportez-vous au [Tableau 6](#) à la page 98.

Vous avez la possibilité de combiner des sauvegardes complètes et incrémentales lorsque vous configurez des sauvegardes planifiées. Vous pouvez, par exemple, réaliser une sauvegarde complète le dimanche et des sauvegardes incrémentales tous les jours ouvrables de la semaine. Pour sauvegarder une grande quantité de données et éviter des flux de données trop importants, nous vous recommandons d'utiliser la méthode de la planification échelonnée. Reportez-vous à la section "[Planification échelonnée de sauvegardes complètes](#)" à la page 116.

## Planification, configurations et sessions de sauvegarde

### Configuration de sauvegarde

Lorsque vous planifiez une sauvegarde, tous les objets indiqués dans la spécification correspondante sont sauvegardés au cours de la session de sauvegarde.

Pour chaque sauvegarde individuelle ou périodique, vous pouvez spécifier les options suivantes : **Type de sauvegarde** (complète ou incrémentale), **Charge réseau** et

**Protection de sauvegarde.** Avec la sauvegarde Split Mirror/Snapshot, dans le cas d'une sauvegarde sur disque ou sur disque + bande avec temps d'indisponibilité nul (restauration instantanée activée), choisissez l'option **Sauvegarde Split Mirror/Snapshot**. Pour la sauvegarde sur disque avec temps d'indisponibilité nul, le type de sauvegarde est ignoré et l'opération réalisée est une sauvegarde complète.

Dans une spécification de sauvegarde, vous pouvez planifier à la fois des sauvegardes avec temps d'indisponibilité nul sur disque et sur disque + bande et indiquer une période de protection des données différente pour chaque sauvegarde individuelle ou planifiée périodiquement.

## Session de sauvegarde

Au lancement d'une session de sauvegarde, Data Protector tente d'allouer toutes les ressources nécessaires, telles que les périphériques. La session reste en file d'attente tant que les ressources minimales requises ne sont pas disponibles. Data Protector tente d'allouer les ressources pendant une période spécifique : le délai d'attente. Vous pouvez configurer ce dernier. Si les ressources ne sont toujours pas disponibles au terme du délai d'attente, la session est abandonnée.

## Optimisation des performances de sauvegarde

Pour optimiser la charge du Gestionnaire de cellule, Data Protector lance par défaut cinq sessions de sauvegarde en même temps. Si un plus grand nombre de sessions simultanées est planifié, les sessions supplémentaires sont mises en file d'attente et lancées une fois les autres terminées.

## Planification - Conseils et pièges à éviter

Les concepts de génération de sauvegarde, de protection des données et de protection de catalogue sont décrits dans les sections "[Sauvegardes complètes et incrémentales](#)" à la page 98 et "[Conservation des données sauvegardées et des informations sur les données](#)" à la page 106.

Vous trouverez dans cette section des illustrations de tous ces concepts sous la forme d'exemples de planifications de sauvegarde, accompagnés de quelques conseils qui vous aideront à planifier efficacement vos sauvegardes.

## Quand planifier des sauvegardes ?

D'une manière générale, planifiez les sauvegardes afin qu'elles s'exécutent lorsque l'activité des utilisateurs est au plus bas, généralement la nuit. Les sauvegardes complètes étant plus longues à réaliser, planifiez-les durant les week-ends.

Pensez à planifier les sauvegardes complètes des différents clients (spécifications de sauvegarde) sur plusieurs jours, comme l'indique la section "[Planification échelonnée de sauvegardes complètes](#)" à la page 116.



#### REMARQUE :

Avec Data Protector, vous pouvez établir des rapports représentant la disponibilité des périphériques par tranches horaires. Vous pouvez ainsi choisir un moment où les périphériques requis ne risquent pas d'être utilisés pour des sauvegardes existantes.

## Planification échelonnée de sauvegardes complètes

Effectuer une sauvegarde complète de l'ensemble des systèmes le même jour risque d'entraîner des problèmes de surcharge réseau et de fenêtre temporelle. Pour éviter cela, il est préférable d'utiliser la méthode de planification échelonnée pour vos sauvegardes complètes.

**Tableau 8 Planification échelonnée**

	Lun	Mar	Mer	...
grp_système_a	COMPL.	Incr. 1	Incr. 1	...
grp_système_b	Incr. 1	COMPL.	Incr. 1	...
grp_système_c	Incr. 1	Incr. 1	COMPL.	...

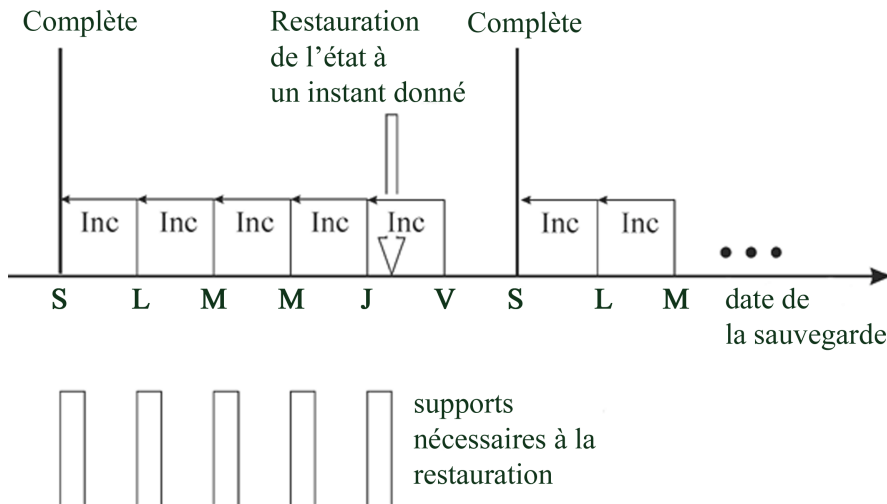
## Optimisation de la restauration

La combinaison de votre stratégie de planification avec des sauvegardes complètes ou incrémentales a une grande incidence sur le temps nécessaire à la restauration des données. Trois exemples sont fournis dans cette section à titre d'illustration.

Pour pouvoir effectuer une restauration de l'état à un instant donné, vous devez disposer d'une sauvegarde complète, ainsi que de toutes les sauvegardes incrémentales réalisées entre cette dernière et l'instant en question. Les sauvegardes complètes et incrémentales n'étant généralement pas effectuées sur les mêmes supports, vous devrez probablement charger différents supports. Pour obtenir des informations complémentaires sur la manière dont Data Protector sélectionne les supports pour les sauvegardes, reportez-vous à la section [Sélection des supports utilisés pour la sauvegarde](#).

## Exemple 1

La Figure 30 à la page 117 illustre une stratégie de planification basée sur une sauvegarde complète associée à des sauvegardes incrémentales simples.

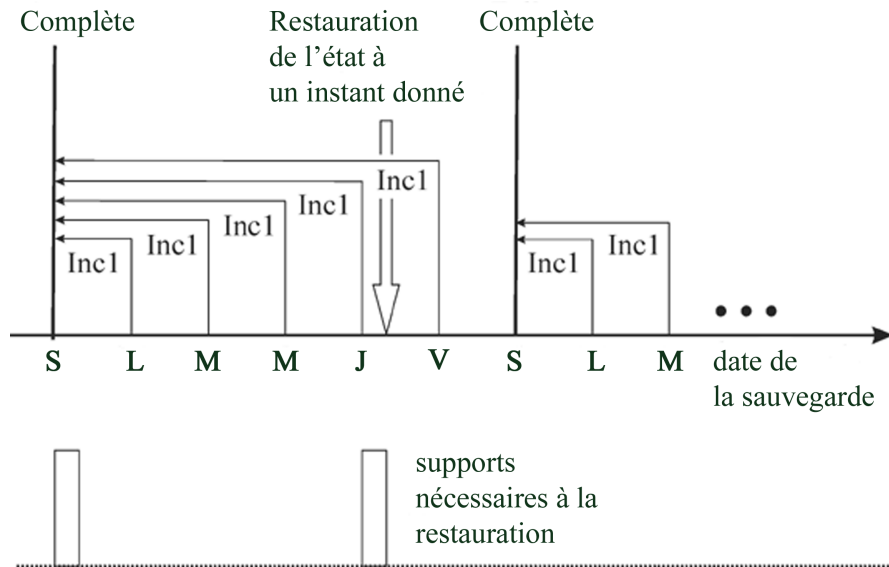


**Figure 30 Sauvegarde complète avec des sauvegardes incrémentales simples quotidiennes**

Cette stratégie permet de réduire l'espace support et le temps nécessaires aux sauvegardes, car seules les modifications effectuées depuis la veille sont prises en compte. Toutefois, pour restaurer des fichiers sauvegardés un jeudi, par exemple, vous aurez besoin des supports utilisés pour la sauvegarde complète, et de tous ceux ayant été utilisés pour les sauvegardes incrémentales effectuées jusqu'au jeudi (dans l'exemple ci-dessus, cinq jeux de supports). Le processus de restauration est par conséquent plus complexe et plus lent.

## Exemple 2

La Figure 31 à la page 118 illustre une stratégie de planification basée sur une sauvegarde complète associée à des sauvegardes incrémentales de niveau un.

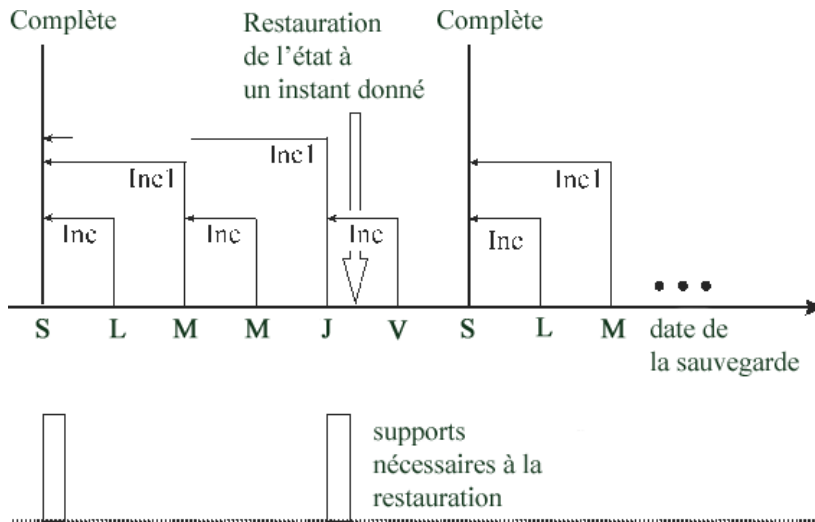


**Figure 31 Sauvegarde complète avec des sauvegardes incrémentales quotidiennes de niveau 1**

Cette stratégie nécessite légèrement plus de temps pour les sauvegardes et requiert un peu plus d'espace support, puisque toutes les modifications effectuées depuis la sauvegarde complète la plus récente sont enregistrées chaque jour. Pour restaurer des fichiers sauvegardés le jeudi, par exemple, vous aurez besoin des supports utilisés pour la sauvegarde complète, ainsi que ceux utilisés pour la sauvegarde incrémentale du jeudi (dans notre cas, deux jeux de supports seulement). Cela permet de simplifier et d'accélérer considérablement le processus de restauration.

### Exemple 3

Selon votre environnement et vos besoins, la meilleure solution peut être un compromis entre ces deux options. Vous pourriez, par exemple, définir la stratégie de planification suivante :



**Figure 32 Sauvegarde complète avec des sauvegardes incrémentales mixtes**

Cette stratégie tient compte du fait que seul un petit nombre de modifications sont effectuées durant le week-end. Les données sont sauvegardées à l'aide d'une combinaison de sauvegardes incrémentales simples et de sauvegardes Incr1 (différentielles), dans le but d'optimiser les performances de la sauvegarde. Pour restaurer des fichiers sauvegardés jeudi, par exemple, vous aurez besoin des supports utilisés pour la sauvegarde complète et de ceux utilisés pour la deuxième sauvegarde Incr1 (dans notre cas, deux jeux de supports).

## Opération automatisée ou sans surveillance

Pour simplifier les opérations et le travail de l'opérateur au cours du processus de sauvegarde, Data Protector fournit des fonctionnalités poussées prenant en charge les sauvegardes sans surveillance ou automatiques pendant les périodes hors activité. Cette section vous explique comment élaborer vos stratégies de planification et dans quelle mesure elles ont une influence sur le comportement de la sauvegarde, et vous donne des exemples de stratégie de planification. Une attention toute particulière est apportée aux longues périodes d'opération sans surveillance (de plusieurs jours à plusieurs semaines), plutôt qu'à l'opération sans surveillance dans le cadre d'une sauvegarde unique.

## A propos des sauvegardes sans surveillance

Data Protector propose des méthodes simples de planification de vos sauvegardes. L'efficacité des stratégies de planification étant liée à votre environnement, il est indispensable de l'analyser avant de rechercher la stratégie de planification la mieux adaptée.

- A quel moment l'utilisation du système et l'activité des utilisateurs sont-elles les plus faibles ?  
C'est généralement pendant la nuit, et c'est à ce moment-là qu'est planifiée l'exécution de la plupart des sauvegardes. Data Protector peut générer des rapports sur les périphériques utilisés pour les sauvegardes.
- De quel type sont les données à traiter et à quelle fréquence souhaitez-vous planifier leur sauvegarde ?  
Les données souvent modifiées et stratégiques pour l'entreprise, telles que les fichiers utilisateur, les transactions et les bases de données, doivent être sauvegardées régulièrement. A l'inverse, il n'est pas nécessaire de sauvegarder souvent les données spécifiques au système, comme les fichiers de programme, qui sont peu susceptibles d'être modifiées.
- Jusqu'à quel point souhaitez-vous simplifier la restauration ?  
Selon la manière dont vous planifiez vos sauvegardes complètes et incrémentales, vous aurez besoin des supports utilisés lors des différentes sauvegardes pour pouvoir restaurer la version la plus récente des fichiers. La procédure peut prendre plus ou moins de temps, voire nécessiter un traitement manuel des supports si vous ne disposez pas d'un périphérique de bibliothèque automatique.
- Quelle quantité de données devez-vous sauvegarder ?  
Les sauvegardes complètes sont plus longues à réaliser que les sauvegardes incrémentales. Les sauvegardes doivent généralement être effectuées dans un intervalle de temps limité.
- Combien de supports sont requis ?  
Définissez une stratégie de rotation des supports. Reportez-vous à la section "[Mise en œuvre d'une stratégie de rotation des supports](#)" à la page 158. Vous saurez ainsi si le nombre de supports pouvant être conservés dans la bibliothèque prévue est suffisant pour effectuer des sauvegardes sur la période définie sans devoir gérer les supports manuellement.
- Comment traiter les invites de montage ?  
Déterminez si vous avez besoin d'utiliser une ou plusieurs bibliothèques. Si vous n'en utilisez qu'une, Data Protector peut alors accéder à la quasi-totalité des



supports, ce qui signifie qu'il peut fonctionner en mode automatique, réduisant ainsi de manière significative les interventions manuelles sur les supports. Si le volume de données à traiter est trop important pour une seule bibliothèque, envisagez d'utiliser plusieurs bibliothèques. Pour plus d'informations, reportez-vous à la section "[Grandes bibliothèques](#)" à la page 179.

- Comment gérer les périphériques non disponibles ?  
Utilisez les fonctions d'équilibrage dynamique des charges, ou chaînage des périphériques, et pensez à définir plusieurs périphériques lors de la création d'une spécification de sauvegarde. Vous éviterez ainsi l'échec d'une sauvegarde dans le cas où un périphérique ne serait pas prêt ou en cas de dysfonctionnement du système auquel le périphérique est connecté.
- Combien de temps peut prendre une sauvegarde de l'ensemble des données ?  
Les sauvegardes devant être effectuées pendant les périodes où l'utilisation du réseau et l'activité des utilisateurs sont faibles, il est indispensable de planifier les sauvegardes de manière à distribuer la charge réseau qui en résulte et à optimiser l'efficacité des sessions de sauvegarde. Vous serez peut-être amené à mettre en place une stratégie de planification échelonnée.  
Si vous avez de grandes quantités de données à sauvegarder et que la fenêtre de sauvegarde présente un problème, envisagez l'utilisation d'un périphérique sur disque pour vos sauvegardes et l'utilisation des stratégies de sauvegarde avancées telles que la sauvegarde synthétique et la sauvegarde de disque en plusieurs étapes.
- Comment préparer les applications en cours d'exécution pour les sauvegardes ?  
Étant donné qu'un grand nombre d'applications gardent les fichiers ouverts, l'exécution d'une sauvegarde entraînerait des incohérences. Pour remédier à cela, utilisez les scripts de pré- et post-exécution qui permettront de synchroniser l'état des applications avec les opérations de sauvegarde.

## Duplication de données sauvegardées

La duplication de données sauvegardées présente plusieurs avantages. Vous pouvez copier des données pour améliorer leur sécurité et leur disponibilité, ou bien à des fins d'utilisation.

Data Protector fournit les méthodes suivantes de duplication des données sauvegardées : copie d'objet, mise en miroir d'objet et copie de support.

Reportez-vous au [Tableau 9](#) à la page 122 pour une vue d'ensemble des principales caractéristiques de ces méthodes.

**Tableau 9 Méthodes de duplication de données Data Protector**

	<b>Copie d'objets</b>	<b>Miroir d'objet</b>	<b>Copie de supports</b>	<b>Copie intelligente de supports</b>
<b>Éléments dupliqués</b>	N'importe quelle combinaison de versions d'objets appartenant à une ou plusieurs sessions de sauvegarde, copie ou consolidation d'objet.	Un ensemble d'objets d'une session de sauvegarde	Un support entier	Un support entier
<b>Temps de duplication</b>	A tout moment à l'issue d'une sauvegarde	Pendant la sauvegarde	A tout moment après une sauvegarde	A tout moment après une sauvegarde
<b>Type de support source et cible</b>	Peut être différent	Peut être différent	Doit être identique	Diffère car le stockage sur disque est combiné au stockage sur bande
<b>Taille des supports sources et cibles</b>	Peut être différent	Peut être différent	Doit être identique	Doit être identique <sup>1</sup>
<b>Ajout de supports cible</b>	Oui	Oui	Non <sup>2</sup>	Non <sup>3</sup>
<b>Résultat de l'opération</b>	Supports contenant les versions d'objet sélectionnées	Supports contenant les versions d'objet sélectionnées	Supports identiques aux supports sources	Supports identiques aux supports sources

<sup>1</sup>Les supports sources sont sur des bandes virtuelles stockées dans des baies de disques et les supports cibles sont dans une bibliothèque de bandes virtuelle connectée au VLS.

<sup>2</sup>Vous ne pouvez utiliser comme supports cibles que des supports non formatés, vierges ou dont la protection a expiré. Après l'opération, aucun ajout n'est possible aux supports sources et cibles.

<sup>3</sup>Vous ne pouvez utiliser comme supports cibles que des supports non formatés, vierges ou dont la protection a expiré. Après l'opération, aucun ajout n'est possible aux supports sources et cibles.

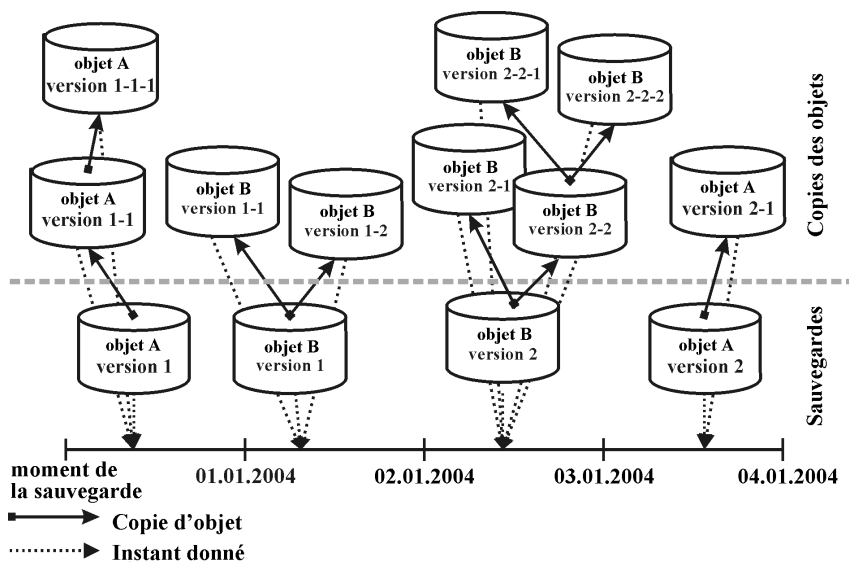
## Copie d'objets

### Qu'est-ce que la copie d'objets ?

La fonctionnalité de copie d'objet de Data Protector vous permet de copier des versions d'objet sélectionnées vers un jeu de supports spécifique. Vous pouvez sélectionner des versions d'objets appartenant à une ou plusieurs sessions de sauvegarde, copie ou consolidation d'objet. Pendant la session de copie d'objet, Data Protector lit les données sauvegardées à partir du support source, les transfère et les écrit sur le support cible.

Une session de copie d'objets produit un jeu de supports contenant des copies des versions d'objet spécifiées.

La [Figure 33](#) à la page 123 indique comment les données sauvegardées à un moment donné peuvent être copiées ultérieurement. Vous pouvez copier un objet sauvegardé à partir d'un support contenant une sauvegarde ou d'un support contenant une copie de l'objet.



**Figure 33** Concept de la copie d'objet

La figure présente une version d'objet résultant d'une sauvegarde de l'objet A, version 1 et deux copies supplémentaires de la même version d'objet. La version 1-1 a été obtenue en copiant une version d'objet résultant de la sauvegarde et la version 1-1-1 en copiant une copie de la version d'objet. N'importe laquelle de ces

versions d'objet peut être utilisée pour effectuer une restauration de la même version d'objet.

### Lancement de la session de copie d'objet

Vous pouvez lancer la session de copie d'objet de manière interactive ou spécifier un lancement automatisé de la session. Data Protector propose deux types de copie d'objet automatisée : la **copie d'objet après sauvegarde** et la **copie d'objet planifiée**.

### Copie d'objets post-sauvegarde

La copie d'objets post-sauvegarde, post-copie et post-consolidation (sous-ensembles de copie d'objets post-sauvegarde) intervient après la fin d'une session définie dans la spécification de copie d'objet automatisée. Elle copie les objets sélectionnés en fonction de la spécification de copie d'objets automatisée, qui ont été écrits au cours de la session concernée.

### Copie d'objets planifiée

La copie d'objets planifiée s'effectue à l'heure définie par l'utilisateur. Les objets de différentes sessions peuvent être copiés au cours d'une même session de copie d'objets planifiée.

### Sélection des périphériques

Vous devez disposer de périphériques distincts pour les supports sources et les supports cibles. Les périphériques de destination peuvent avoir une taille de bloc supérieure aux périphériques source. Toutefois, pour éviter toute incidence négative sur les performances, il est recommandé d'utiliser des périphériques ayant la même taille de bloc et étant reliés au même système ou à un environnement SAN.

Par défaut, le partage de charge est appliqué à la copie d'objet. Data Protector tente d'optimiser l'utilisation des périphériques disponibles en employant le nombre maximum possible de périphériques.

### Sélection de périphériques sources

Par défaut, Data Protector sélectionne automatiquement les périphériques sources pour une copie d'objet selon les stratégies de périphérique définies dans la configuration des périphériques. Ceci garantit une utilisation optimale des ressources disponibles. Vous pouvez désactiver la sélection automatique de périphérique si vous voulez utiliser le périphérique d'origine ou sélectionner un périphérique spécifique :

- Sélection automatique des périphériques (par défaut)

Data Protector utilise automatiquement le périphérique source disponible. Ce périphérique est sélectionné pour une copie d'objet. Il est de même type (par exemple, LTO) et provient de la même bibliothèque que le périphérique d'origine qu'il remplace.

Data Protector essaye d'abord d'utiliser le périphérique qui a été utilisé pour l'écriture de l'objet (le périphérique d'origine). Si ce dernier n'est pas sélectionné pour une copie d'objet, une variable globale est prise en compte. Pour que Data Protector utilise un autre périphérique en premier ou pour qu'il n'utilise pas le périphérique d'origine, modifiez la variable globale `AutomaticDeviceSelectionOrder`.

Vous pouvez rassembler des périphériques dans des groupes de périphériques pour des utilisations différentes en spécifiant une balise de périphérique. Les périphériques portant la même balise sont considérés comme compatibles et peuvent se substituer les uns aux autres. Les périphériques d'origine non disponibles peuvent être remplacés par les périphériques qui portent la même balise et qui proviennent de la même bibliothèque. Par défaut, aucune balise de périphérique n'est définie.

Notez que si le périphérique d'origine est supprimé, un périphérique de la même bibliothèque et du même type le remplace. Que ce périphérique soit sélectionné pour une copie d'objet ou qu'il ait la même balise que le périphérique d'origine n'a pas d'importance.

Vous pouvez lancer la copie d'objet avec moins de périphériques que pour la sauvegarde.

- Sélection des périphériques d'origine

Data Protector utilise le périphérique d'origine comme périphérique source pour une copie d'objet et attend si ce dernier n'est pas disponible.

### Sélection des périphériques de destination

Si les périphériques de destination ne sont pas spécifiés par objet, Data Protector les sélectionne automatiquement parmi ceux que vous avez choisis dans la spécification de copie d'objet, en fonction des critères suivants et par ordre de priorité :

- Les périphériques de destination ayant la même taille de bloc que les périphériques sources sont sélectionnés avant ceux dont la taille de bloc diffère.
- Les périphériques connectés localement sont sélectionnés avant les périphériques en réseau.

Les périphériques sont verrouillés au début de la session. Les périphériques non disponibles à ce moment-là ne pourront pas être utilisés pendant la session puisque le verrouillage des périphériques ne peut pas être effectué une fois la session

commencée. Si une erreur survient au niveau du support, le périphérique concerné ne doit pas être utilisé pendant la session de copie.

### Sélection du jeu de supports depuis lequel effectuer la copie

Si vous souhaitez copier une version d'objet existant sur plusieurs jeux de supports et ayant été créée par le biais d'une méthode de duplication de données Data Protector, n'importe lequel des jeux de supports peut être utilisé en tant que source pour la copie. Vous pouvez influencer sur la sélection des jeux de supports en spécifiant la priorité des emplacements des supports.

Le processus global de sélection des supports est le même que pour la restauration. Pour plus de détails, reportez-vous à la section "[Sélection du jeu de supports](#)" à la page 139.

### Performances d'une session de copie d'objet

D'autres facteurs, tels que les tailles de bloc d'un périphérique et la connexion de périphériques, peuvent également affecter les performances de copie d'objet. Si les périphériques participant à la session de copie d'objet présentent des tailles de bloc différentes, les données seront regroupées pendant la session, ce qui demande plus de temps et monopolise davantage de ressources. Si les données sont transférées via le réseau, cela implique une charge supplémentaire pour le réseau et une durée d'opération plus longue. Il est possible de minimiser cet impact en utilisant le partage de charge pour cette opération.

### Pourquoi utiliser la fonction de copie d'objet ?

D'autres copies des données sauvegardées, copiées ou consolidées sont créées à des fins diverses et variées :

- Mise au coffre  
Vous pouvez créer des copies d'objets sauvegardés, copiés ou consolidés et les conserver à plusieurs emplacements.
- Libération de supports  
Pour ne conserver que des versions d'objet protégées sur des supports, vous pouvez copier ces versions d'objet, puis libérer le support à des fins d'écrasement.
- Démultiplexage des supports  
Vous pouvez copier des objets pour éliminer l'entrelacement des données.
- Regroupement d'une chaîne de restauration  
Vous pouvez copier toutes les versions d'objet nécessaires pour une restauration vers un seul jeu de supports.

- Migration vers un autre type de support  
Vous pouvez copier vos sauvegardes sur des supports de différents types.
- Prise en charge de concepts de sauvegarde avancés  
Vous pouvez utiliser des concepts de sauvegarde tels que la sauvegarde de disque en plusieurs étapes.

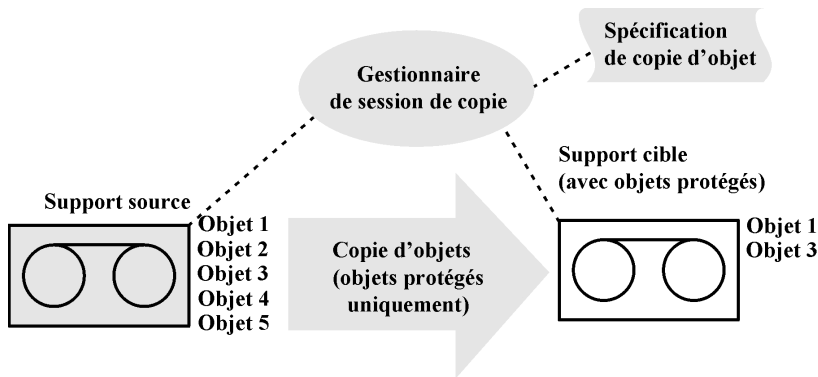
### Mise au coffre

La mise au coffre est un processus de stockage des supports dans un lieu sûr, souvent appelé coffre, où ils peuvent être conservés pendant une période donnée. Pour plus de détails, reportez-vous à la section “[Mise au coffre](#)” à la page 168.

Il est recommandé de conserver une copie des données sauvegardées sur site à des fins de restauration. Pour obtenir des copies supplémentaires, vous pouvez utiliser la copie d'objet, la mise en miroir d'objet ou la fonction de copie de supports, selon vos besoins.

### Libération de supports

Vous pouvez réduire le nombre de supports utilisés en ne conservant que les sauvegardes protégées et en écrasant les autres. Un support pouvant contenir aussi bien des sauvegardes protégées que non protégées, vous pouvez copier des objets protégés sur un nouveau jeu de supports et écraser les autres. Reportez-vous à la [Figure 34](#) à la page 127.



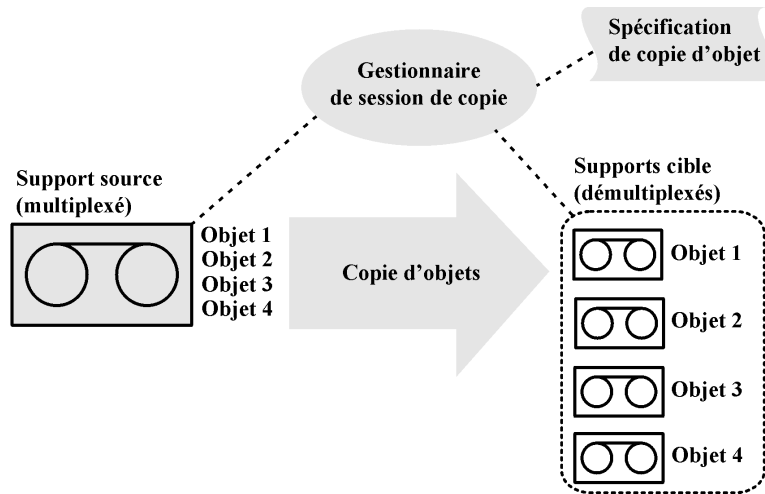
**Figure 34 Libération de supports**

### Démultiplexage des supports

Les supports multiplexés peuvent contenir des données entrelacées de plusieurs objets. Ces supports peuvent provenir de sessions de sauvegarde dont la simultanéité des

périphériques est supérieure à 1. Les supports multiplexés compromettent la confidentialité des sauvegardes et la restauration est plus longue.

Data Protector permet de démultiplexer les supports. Les objets provenant d'un support multiplexé sont copiés sur les différents supports que vous spécifiez. Reportez-vous à la [Figure 35](#) à la page 128.



**Figure 35** Démultiplexage d'un support

### Regroupement d'une chaîne de restauration

Vous pouvez copier la chaîne de restauration (toutes les sauvegardes nécessaires pour une restauration) d'une version d'objet sur un nouveau jeu de supports. Une restauration effectuée à partir de ce type de jeu de supports est plus rapide et plus pratique. En effet, il n'est pas nécessaire de charger plusieurs supports et de rechercher les versions d'objet nécessaires.

### Migration vers un autre type de support

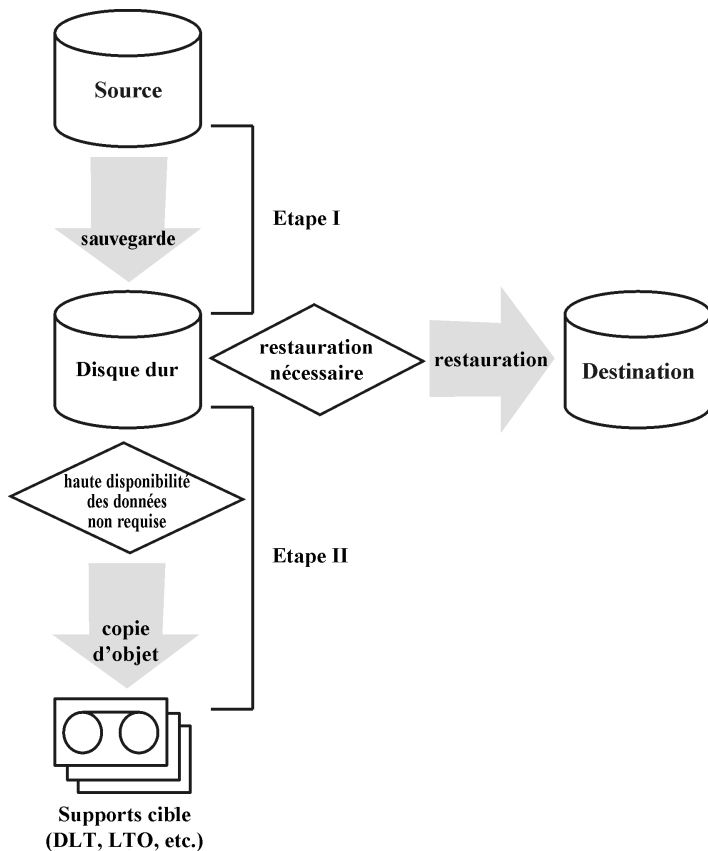
Vous pouvez migrer les données sauvegardées vers un autre type de support. Vous pouvez par exemple copier des objets à partir de périphériques de fichier vers des périphériques LTO ou de périphériques DLT vers des périphériques LTO.

### Sauvegarde de disque en plusieurs étapes

Le concept de sauvegarde de disque en plusieurs étapes permet d'améliorer les performances des sauvegardes et des restaurations, de réduire les coûts de stockage des données sauvegardées et d'augmenter la disponibilité et l'accessibilité des données pour la restauration.



Les étapes de la sauvegarde consistent à sauvegarder des données sur des supports d'un certain type, puis à les déplacer vers des supports d'un type différent. Les données sont sauvegardées vers des supports caractérisés par de hautes performances et une grande accessibilité, mais par des capacités limitées (par exemple, des disques système). Ces sauvegardes restent généralement accessibles à la restauration pendant la période où ce type d'opération est le plus probable. Après un certain temps, les données sont déplacées vers des supports dont les performances et l'accessibilité sont moins élevées mais dont les capacités de stockage sont importantes, au moyen de la fonction de copie d'objet. Reportez-vous à la [Figure 36](#) à la page 129.



**Figure 36** Concept de sauvegarde de disque en plusieurs étapes

Ce processus peut être réalisé comme une opération automatisée.

L'exemple ci-dessous décrit brièvement une approche facile à mettre en œuvre en tant qu'opération standard et offrant une sécurité supplémentaire au niveau des données. Il utilise des options pour définir la protection des données sources et cibles

de manière indépendante. Les conditions sont les suivantes : restauration rapide à partir du disque pendant les 15 premiers jours, puis restauration standard à partir de la bande pendant 30 jours supplémentaires.

- La sauvegarde initiale est une sauvegarde sur disque via une bibliothèque de fichiers et la protection des données et du catalogue est de 45 jours (conditions globales).
- La sauvegarde est suivie d'une opération de copie pendant laquelle les objets de sauvegarde sont copiés sur bande, la sauvegarde initiale restant dans la bibliothèque de fichiers. Si la copie sur bande est correctement réalisée, la protection des données et du catalogue correspondante est de 45 jours.
- Comme une copie correcte a été créée, la durée de la protection pour la sauvegarde sur disque peut être réduite à 15 jours, période pendant laquelle la restauration rapide est requise. Après cette période, elle peut être supprimée et la copie sur bande est utilisée pour la sécurité à plus long terme. Jusqu'à ce moment, la copie sur bande offre une sécurité supplémentaire au cas où la copie sur disque serait endommagée.

La sauvegarde de disque en plusieurs étapes élimine également le besoin d'effectuer fréquemment des sauvegardes sur bande de nombreux objets de petite taille. Ces sauvegardes sont inadaptées en raison de la fréquence élevée des chargements et déchargements des supports. L'utilisation de la sauvegarde de disque en plusieurs étapes réduit les temps de sauvegarde et empêche la détérioration des supports.

## Mise en miroir d'objets

### Qu'est-ce que la mise en miroir d'objets ?

La fonction de mise en miroir d'objet Data Protector permet d'écrire simultanément les mêmes données sur plusieurs jeux de supports pendant une session de sauvegarde. Vous pouvez mettre en miroir tout ou partie des objets sauvegarde sur un ou plusieurs jeux de supports supplémentaires.

Le résultat d'une session de sauvegarde réussie avec miroir d'objet est un jeu de supports contenant les objets sauvegardés et des jeux de supports supplémentaires contenant les objets mis en miroir. Les objets mis en miroir sur ces supports sont considérés comme des copies d'objets.

### Avantages de la mise en miroir d'objets

La fonction de mise en miroir d'objets répond aux besoins suivants :

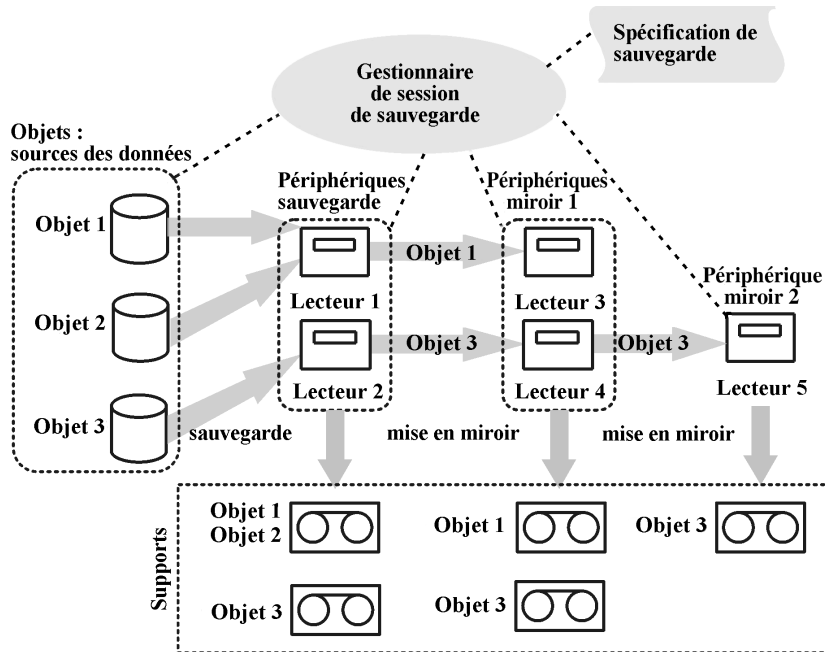
- Elle augmente la disponibilité des données sauvegardées du fait de l'existence de plusieurs copies.

- Elle permet une mise au coffre aisée sur plusieurs sites puisque les données sauvegardées peuvent être mises en miroir sur des sites distants.
- Elle améliore la tolérance aux pannes des sauvegardes puisque les données sont écrites sur plusieurs supports. Un incident au niveau d'un support n'affecte pas la création des autres miroirs.

### Opération de mise en miroir d'objets

Dans une session de sauvegarde avec mise en miroir d'objets, chaque objet sélectionné est sauvegardé et mis en miroir simultanément autant de fois que spécifié dans la spécification de sauvegarde. Reportez-vous à la [Figure 37](#) à la page 132.

Prenons comme exemple l'Objet 3 de la figure. L'Agent de disque lit un bloc de données à partir du disque et l'envoie vers l'Agent de support responsable de la sauvegarde de l'objet. L'Agent de support écrit les données sur le support du Lecteur 2 et les transmet à l'Agent de support responsable du miroir 1. Ce dernier écrit à son tour les données sur le support du Lecteur 4 et les transmet à l'Agent de support responsable du miroir 2. Celui-ci écrit les données sur le support du Lecteur 5. A la fin de la session, l'Objet 3 est disponible sur trois supports.



**Figure 37 Mise en miroir d'objets**

### Sélection des périphériques

Par défaut, le partage de charge est appliqué à la mise en miroir d'objets. Data Protector tente d'optimiser l'utilisation des périphériques disponibles en employant autant de périphériques que possible. Les périphériques sont sélectionnés en fonction des critères suivants, par ordre de priorité :

- Des périphériques de la même taille de bloc sont sélectionnés s'ils sont disponibles.
- Les périphériques connectés localement sont sélectionnés avant les périphériques en réseau.

Quand vous effectuez une opération de mise en miroir d'objets à partir de la ligne de commande, la fonction de partage de charge n'est pas disponible.

### Performances de la sauvegarde

La mise en miroir d'objets a une incidence sur les performances de sauvegarde. Sur les clients Gestionnaire de cellule et Agents de support, l'impact de l'écriture de miroirs est le même que celui de la sauvegarde d'objets supplémentaires. Sur ces systèmes, les performances de sauvegarde diminuent en fonction du nombre de miroirs.

Sur les clients Agents de disque, la mise en miroir ne provoque aucun impact, car les objets sauvegarde ne sont lus qu'une fois.

Les performances de sauvegarde dépendent également de facteurs tels que la taille de bloc et la connexion des périphériques. Si les périphériques utilisés pour la sauvegarde et la mise en miroir d'objets ont des tailles de bloc différentes, les données enregistrées dans les miroirs sont réassemblées durant l'opération, ce qui demande davantage de temps et de ressources. Si les données sont transférées via le réseau, cela implique une charge supplémentaire pour le réseau et une durée d'opération plus longue.

## Copie de supports

### Qu'est-ce que la copie de supports ?

La fonctionnalité de copie de supports Data Protector vous permet de copier des supports après l'exécution d'une sauvegarde. La procédure de copie d'un support consiste à créer une copie exacte d'un support de sauvegarde. Elle permet de dupliquer un support à des fins d'archivage ou de mise au coffre. Une fois le support copié, vous pouvez transférer l'original ou la copie vers un site de mise au coffre.

Il est possible de copier des supports manuellement ou de configurer Data Protector pour que la copie soit effectuée automatiquement. Pour plus de détails, reportez-vous à la section "[Copie automatisée des supports](#)" à la page 135.

### Comment copier des supports ?

Vous devez disposer de deux périphériques utilisant le même type de support, l'un pour le support source et l'autre pour le support cible. Le support source correspond au support à copier, et le support cible à celui sur lequel les données sont copiées.

Lorsque vous copiez des supports au sein d'une bibliothèque possédant plusieurs lecteurs, vous pouvez utiliser un lecteur pour la source et un autre pour la copie.

### Quel est le résultat ?

La copie de supports résulte en deux jeux de supports identiques, à savoir le jeu de supports d'origine et sa copie. L'un ou l'autre peut être utilisé pour la restauration.

Une fois le support source copié, Data Protector lui attribue la propriété Sans ajout possible, afin d'éviter que de nouvelles données de sauvegarde ne soient écrites sur ce support (l'original serait alors différent de sa copie). La copie se voit également attribuer la propriété Sans ajout possible. Par défaut, le paramètre de protection de la copie est identique à celui de l'original.

Vous pouvez réaliser plusieurs copies du support d'origine. Toutefois, vous ne pouvez pas faire des copies de copies, également connues sous le nom de copies de deuxième génération.

## Copie automatisée des supports

### Qu'est-ce que la copie automatisée des supports ?

La copie automatisée des supports est une procédure de création automatique de copies de supports de sauvegarde. Cette fonctionnalité est disponible en cas d'utilisation de périphériques de bibliothèque.

Deux types de procédures de copie automatisée sont disponibles dans Data Protector : les procédures de copie après sauvegarde et avant sauvegarde.

### Copie de supports post-sauvegarde

La copie de supports après sauvegarde est effectuée une fois la session de sauvegarde terminée. Les supports copiés sont ceux utilisés lors de la session en question.

### Copie de supports planifiée

La copie de supports planifiée est effectuée à l'heure définie par l'utilisateur. Il est possible de copier en une seule session des supports régis par des spécifications de sauvegarde différentes. Pour définir les supports à copier, vous créez une spécification de copie automatisée des supports.

### Comment la copie automatisée des supports fonctionne-t-elle ?

Vous créez d'abord une spécification de copie automatisée des supports. Lorsque la session de copie automatisée des supports débute, Data Protector génère une liste de supports, appelés supports sources, en fonction des paramètres indiqués dans la spécification de copie automatisée des supports. Pour chaque support source, Data Protector sélectionne le support cible sur lequel les données seront copiées. Les supports cibles sont sélectionnés dans le même pool de supports que le support source, dans un pool libre ou parmi les supports vierges de la bibliothèque.

Pour chaque support source, Data Protector sélectionne deux périphériques parmi ceux indiqués au niveau de la spécification de copie automatisée des supports. La fonction de copie automatisée des supports effectue elle-même le partage de la charge, selon les besoins. Pour une exploitation optimale des périphériques, Data Protector utilise autant de périphériques que possible et sélectionne de préférence des périphériques installés en local.

La fonction de copie automatisée des supports ne gère pas les demandes de montage ou "cleanme". En cas de réception d'une demande de montage, l'utilisation des deux supports concernés est abandonnée mais la session continue.

Pour obtenir des exemples d'utilisation, reportez-vous à la section "[Exemples de copie automatisée des supports](#)" à la page 356.

## Copie intelligente de supports avec VLS

### Qu'est-ce que la copie intelligente de supports (Smart Media copying) ?

Lors du processus de copie des supports intelligente, les données sont d'abord sauvegardées sur une bibliothèque de bandes virtuelle configurée sur le Virtual Library System (VLS). Ensuite, une bande virtuelle contenant une sauvegarde est copiée dans la bibliothèque physique reliée au VLS au cours d'un processus appelé auto-migration. Data Protector lance le processus de copie, qui est alors effectué par le VLS. Les données sont transférées à une bibliothèque physique par une opération de copie intelligente, qui permet à Data Protector de distinguer le support source et le support cible et donc de gérer les supports. Les supports de copie intelligente suivent le format Data Protector ; ils peuvent donc être insérés dans tout lecteur de bande compatible et lus par Data Protector. La copie intelligente donne lieu à deux jeux de supports identiques, le support source qui se trouve sur la bande virtuelle du VLS et le support cible (une copie intelligente) situé dans une bibliothèque de bandes virtuelle reliée au VLS. N'importe laquelle de ces copies peut être utilisée pour la restauration, la sécurité et la disponibilité des données sauvegardées étant ainsi renforcées. Vous pouvez également conserver des copies intelligentes de supports à des fins d'archivage ou de mise au coffre.

Deux types de procédures de copie des supports intelligente sont disponibles dans Data Protector : copie des supports intelligente automatisée et copie des supports intelligente interactive.

### Copie des supports intelligente automatisée

Vous pouvez créer les copies de supports intelligentes automatisées suivantes :

- Copie de supports intelligente après sauvegarde, qui intervient une fois la session de sauvegarde terminée et qui copie les supports utilisés dans cette session particulière.
- Copie intelligente de supports planifiée, qui a lieu à une heure spécifique ou à des intervalles réguliers.

## Copie des supports intelligente interactive

La copie des supports intelligente interactive crée une copie d'un support contenant les données sauvegardées et peut être lancé sur demande à tout moment.

## Que se passe-t-il après la sauvegarde ?

Une fois transférées dans la bande physique, les données sauvegardées sont toujours disponibles pour la restauration Data Protector. Toutefois, comme Data Protector ne voit pas la bibliothèque cible, la restauration ne s'effectue pas directement à partir de cette bibliothèque, mais à partir d'un lecteur de bande ou d'une bibliothèque contrôlé par Data Protector.

Pour plus d'informations sur les copies intelligentes du VLS, recherchez l'entrée suivante dans l'index de l'aide en ligne : "copie de supports intelligente" et consultez la documentation du VLS.

# Vérification des supports et des objets de sauvegarde

En tant qu'administrateur de sauvegarde, vous ne pouvez pas vous contenter de sauvegarder régulièrement vos données importantes. Il est tout aussi important que vous soyez sûr de pouvoir restaurer les données sauvegardées en cas de problèmes, particulièrement avec certaines techniques de sauvegarde plus sophistiquées existant actuellement. Avec la fonctionnalité de vérification des supports et des objets de Data Protector, vous pouvez définir différents niveaux de confiance pour la fonctionnalité de restauration.

## Qu'est-ce que la vérification de support ?

Dans Data Protector, l'opération de vérification d'un support permet de savoir si le format des données qu'il contient est correct et de mettre à jour les informations concernant ce support dans la base de données interne. Vous pouvez l'utiliser pour effectuer une vérification interactive de n'importe quel support résident Data Protector complet, unique. Vous pouvez avoir besoin de vérifier les supports dans les cas suivants :

- Vous avez copié un support à des fins d'archivage et vous souhaitez vérifier la validité de la copie avant sa mise au coffre.
- Un support de sauvegarde est plein et vous souhaitez vérifier tous les objets qu'il contient avant son stockage à long terme.



## Que vous apporte la vérification de supports ?

Lorsque vous vérifiez des supports, Data Protector :

- Vérifie l'identification des supports, leur description et les informations d'emplacement dans les en-têtes de Data Protector
- Lit tous les blocs du support et vérifie leur format
- Si l'option CRC (contrôle de redondance cyclique) a été utilisée pour la sauvegarde, Data Protector recalcule le CRC et le compare à celui enregistré sur le support.

La réussite des deux premières vérifications confirme que la bande est dans un état matériel satisfaisant et que toutes les données qu'elle contient ont pu être lues. Elle correspond à un niveau de confiance moyen dans la capacité de restauration de ce support.

Si la troisième vérification réussit, cela confirme que les données de sauvegarde elles-mêmes sont régulières au sein de chaque bloc. Le niveau de confiance dans la capacité de restauration de ce support est élevé.

## Qu'est-ce que la vérification d'objets ?

Dans Data Protector, la vérification d'objets vous permet de contrôler la validité des objets de sauvegarde, par opposition aux supports de sauvegarde. Vous pouvez l'utiliser pour vérifier les points suivants :

- un objet unique ou plusieurs objets
- un support unique ou plusieurs supports
- de manière interactive, ou dans des sessions planifiées ou post-fonctionnement

Vous pouvez utiliser la vérification d'objet :

- après une procédure de copie d'objet sur un autre support
- après une procédure de consolidation d'objet sur la chaîne de restauration d'un objet sauvegardé de manière incrémentale
- pour vérifier tous les objets de sauvegarde produits au cours d'une période donnée après un changement de périphérique de sauvegarde

## Que vous apporte la vérification d'objets ?

Lorsque vous effectuez une procédure de vérification d'objets, Data Protector assure les mêmes niveaux de vérification des données que la procédure de vérification des

supports. Toutefois, alors qu'avec la vérification des supports il peut uniquement contrôler des supports complets uniques, avec la vérification d'objets il peut par exemple vérifier :

- un objet de sauvegarde unique, sans qu'il soit nécessaire de vérifier le support dans son entier, ce qui permet de gagner un temps considérable avec les supports de sauvegarde volumineux
- des objets volumineux qui s'étendent sur plusieurs supports
- plusieurs objets sur plusieurs supports
- une version d'objet spécifique (interactive uniquement)

En outre, vous pouvez exécuter la vérification sur :

- l'hôte de l'Agent de support, ce qui évite de générer du trafic réseau
- un autre hôte, en prenant en compte les effets sur le réseau

Des informations sur les sessions et les spécifications de vérification d'objet se trouvent dans différents rapports sur les spécifications de sessions et sur les sessions d'une période.

## Restauration des données

Les stratégies de restauration des données jouent un rôle essentiel dans la stratégie de sauvegarde globale de votre entreprise. N'oubliez pas ce qui suit :

- Sauvegarder et restaurer des fichiers revient à peu de chose près à en faire une copie. Assurez-vous par conséquent que seules les personnes autorisées disposent des droits nécessaires à la restauration des données confidentielles.
- Assurez-vous que les personnes non autorisées ne puissent pas restaurer les fichiers d'autres personnes.

Dans cette section, nous décrivons plusieurs mises en œuvre de stratégie de restauration avec Data Protector. Vous pouvez restaurer vos données de système de fichiers en parcourant les objets ou les sessions de restauration. Par défaut, les données sont restaurées à leur emplacement d'origine. Vous pouvez toutefois spécifier l'emplacement de destination de votre choix pour les données restaurées.

## Durée de la restauration

En cas de perte de données, l'accès aux données n'est possible qu'au terme du processus de récupération. Il est généralement crucial de réduire au minimum la durée de la restauration de manière à ce que les utilisateurs puissent travailler

normalement. Il est par conséquent recommandé d'évaluer le temps nécessaire à la restauration de données spécifiques.

### Facteurs ayant une influence sur la durée de la restauration

La durée de la restauration dépend d'un certain nombre de facteurs, tels que :

- La quantité de données à restaurer. Ce paramètre a une influence directe sur l'ensemble des éléments suivants.
- La combinaison de sauvegardes complètes et incrémentales choisie. Pour plus de détails, reportez-vous à la section "[Sauvegardes complètes et incrémentales](#)" à la page 98.
- Les supports et les périphériques utilisés pour la sauvegarde. Pour plus de détails, reportez-vous au [Chapitre 3](#) à la page 147.
- La vitesse de fonctionnement des réseaux et systèmes. Pour plus de détails, reportez-vous à la section "[Analyse et planification des performances](#)" à la page 69.
- L'application que vous voulez récupérer, par exemple, des fichiers de base de données Oracle. Pour plus d'informations, reportez-vous au *Guide d'intégration HP Data Protector* approprié.
- L'utilisation de la restauration parallèle. Selon la méthode de sauvegarde des données, plusieurs objets peuvent être restaurés au moyen d'une seule opération de lecture. Reportez-vous à la section "[Restaurations parallèles](#)" à la page 247.
- Vitesse et simplicité de sélection des données à restaurer - ceci dépend des paramètres de niveau de journalisation utilisés au cours de la sauvegarde et de la durée de protection de catalogue. Reportez-vous à la section "[Niveau de journalisation comme paramètre clé réglable de l'IDB](#)" à la page 221.

### Sélection du jeu de supports

Si vous souhaitez restaurer une version d'objet existant sur plusieurs jeux de supports et ayant été créée par le biais d'une méthode de duplication des données Data Protector, n'importe lequel des jeux de supports peut être utilisé pour la restauration. Par défaut, Data Protector sélectionne automatiquement le jeu de supports qui sera utilisé. Vous pouvez influencer sur la sélection des jeux de supports en spécifiant la priorité des emplacements des supports. Vous pouvez également sélectionner manuellement le jeu de supports que vous souhaitez utiliser pour la restauration, sauf en cas de restauration d'objets d'intégration.

## Algorithme de sélection des jeux de supports

Par défaut, Data Protector sélectionne le jeu de supports caractérisé par les meilleurs niveaux de qualité et de disponibilité. Par exemple, Data Protector évite les jeux de supports dont les supports sont manquants ou médiocres ; il prend en compte l'état d'exécution des objets, la disponibilité et l'emplacement du périphérique à utiliser avec un jeu de supports donné, etc. Un jeu de supports situé dans une bibliothèque est utilisé avant celui situé dans un périphérique autonome.

## Sélection de la chaîne de restauration

Si vous utilisez la sauvegarde synthétique, il existe souvent plusieurs chaînes de restauration pour le même point dans le temps. Par défaut, Data Protector sélectionne la chaîne de restauration la plus pratique et les supports les plus appropriés de cette chaîne.

## Priorité des emplacements des supports

Pour influencer sur la sélection des jeux de supports, spécifiez la priorité des emplacements des supports. Ce paramètre est important si vous utilisez le concept de stockage sur plusieurs sites. Si vous conservez des supports sur plusieurs sites, vous pouvez spécifier l'emplacement le mieux adapté à une restauration spécifique. Data Protector utilisera le jeu de supports dont la priorité est la plus élevée si plusieurs jeux de supports correspondent aux conditions de l'algorithme de sélection.

Vous pouvez définir la priorité des emplacements des supports d'une manière générale ou pour une session de restauration spécifique.

## Sélection des périphériques

Par défaut, Data Protector sélectionne automatiquement les périphériques pour une restauration selon les stratégies de périphérique définies dans la configuration des périphériques. Ceci garantit une utilisation optimale des ressources disponibles. Vous pouvez désactiver la sélection automatique de périphérique si vous voulez utiliser le périphérique d'origine ou sélectionner un périphérique spécifique :

- Sélection automatique des périphériques (par défaut)  
Data Protector utilise automatiquement le périphérique disponible. Ce périphérique est sélectionné pour une restauration. Il est de même type (par exemple, LTO) et provient de la même bibliothèque que le périphérique d'origine qu'il remplace.  
Data Protector essaie d'abord d'utiliser le périphérique qui a été utilisé pour l'écriture de l'objet (le périphérique d'origine). Si ce dernier n'est pas sélectionné pour une restauration, une variable globale est prise en compte. Pour que Data Protector utilise un autre périphérique en premier ou pour qu'il n'utilise pas le

périphérique d'origine, modifiez la variable globale AutomaticDeviceSelectionOrder.

Vous pouvez rassembler des périphériques dans des groupes de périphériques pour des utilisations différentes en spécifiant une balise de périphérique. Les périphériques portant la même balise sont considérés comme compatibles et peuvent se substituer les uns aux autres. Les périphériques d'origine non disponibles peuvent être remplacés par les périphériques qui portent la même balise et qui proviennent de la même bibliothèque. Par défaut, aucune balise de périphérique n'est définie.

Notez que si le périphérique d'origine est supprimé, un périphérique de la même bibliothèque et du même type le remplace. Que ce périphérique soit sélectionné pour une restauration ou qu'il ait la même balise que le périphérique d'origine n'a pas d'importance.

Vous pouvez lancer la restauration avec un nombre de périphériques inférieur à celui de la sauvegarde.

- Sélection des périphériques d'origine  
Data Protector utilise le périphérique d'origine pour une restauration et attend si ce dernier n'est pas disponible. Il s'agit de l'option privilégiée pour les intégrations Data Protector SAP MaxDB, IBM UDB DB2, Microsoft SQL Server et Microsoft SharePoint Portal Server. De telles bases de données sont en général sauvegardées avec des flux de données interdépendants, la restauration devant donc être lancée avec le même nombre de périphériques que pour la sauvegarde.

## Opérateurs autorisés à restaurer les données

La stratégie de restauration courante veut que seuls les opérateurs de sauvegarde dédiés ou les administrateurs réseau disposent des droits nécessaires pour effectuer des restaurations de fichiers ou des récupérations après sinistre.

### Quand utiliser cette stratégie ?

Vous pouvez recourir à cette stratégie dans les cas suivants :

- Dans les grands environnements réseau, où il est préférable qu'une personne dédiée s'occupe de ces tâches.
- Dans les environnements où les utilisateurs finaux n'ont pas les connaissances informatiques nécessaires pour effectuer les restaurations de fichiers : des opérateurs certifiés peuvent alors être chargés de la restauration des données sensibles.

## Actions requises

Pour mettre en œuvre cette stratégie, procédez comme suit :

- Ajoutez au groupe d'utilisateurs **opérateurs** ou **admin** Data Protector les opérateurs de sauvegarde ou les administrateurs réseau chargés de restaurer les données d'autres personnes.

Il n'est pas nécessaire d'ajouter d'autres personnes (telles que les utilisateurs qui souhaitent effectuer des opérations de restauration sur leur propre système) à quelque groupe d'utilisateurs Data Protector que ce soit.

- Lors de l'installation, n'installez pas l'interface Data Protector sur les systèmes des utilisateurs finaux. Installez l'Agent de disque permettant à Data Protector de sauvegarder ces systèmes.
- Elaborez une stratégie de traitement des demandes de restauration. Celle-ci doit préciser la manière dont les utilisateurs finaux doivent formuler les demandes de restauration des fichiers, par exemple, via un message électronique contenant toutes les informations dont l'opérateur a besoin pour localiser les fichiers et les restaurer sur le système de l'utilisateur final. Prévoyez également un moyen qui permette aux utilisateurs finaux d'être informés lorsque les fichiers ont été restaurés.

## Utilisateurs finaux autorisés à restaurer les données

Une autre stratégie de restauration consiste à autoriser tous les utilisateurs finaux ou uniquement ceux qui ont été sélectionnés à restaurer leurs propres données. Cette stratégie permet d'assurer une sécurité suffisante et d'épargner à l'opérateur de sauvegarde un certain nombre d'opérations de restauration.

### Quand utiliser cette stratégie ?

Vous pouvez recourir à cette stratégie dans les cas suivants :

- Lorsque les utilisateurs ont des connaissances suffisantes pour pouvoir effectuer les restaurations. Vous pourrez avoir besoin de les former aux principes de base de la sauvegarde et aux opérations de restauration.
- Utilisez les périphériques de sauvegarde de la bibliothèque contenant les supports où sont stockées les sauvegardes les plus récentes. Par défaut, les membres du groupe `utilisateurs finaux` de Data Protector ne sont pas autorisés à traiter les demandes de montage relatives aux supports requis. L'assistance de l'opérateur de sauvegarde sera nécessaire en cas de demandes de montage. Pour éviter cela, utilisez de grandes bibliothèques.

## Actions requises

Pour mettre en œuvre cette stratégie, procédez comme suit :

- Ajoutez au groupe `utilisateurs_finaux` de Data Protector les utilisateurs finaux qui seront autorisés à restaurer leurs données. Pour plus de sécurité, vous pouvez limiter l'accès Data Protector de ces utilisateurs à un système particulier.
- Installez l'interface Data Protector sur les systèmes dont les utilisateurs finaux se servent. Data Protector vérifie automatiquement les droits utilisateur et n'autorise que la fonctionnalité de restauration.
- Lorsque vous configurez les sauvegardes des systèmes des utilisateurs finaux, activez l'option **Public** de Data Protector pour autoriser les utilisateurs finaux à les voir.

## Récupération après sinistre

Cette section est une présentation brève et non exhaustive des concepts de récupération après sinistre. Vous trouverez une description détaillée de la récupération après sinistre (planification, préparation et procédures) dans le *Guide de récupération après sinistre HP Data Protector*.

Un **sinistre informatique** fait référence à un événement ayant pour conséquence de rendre un système informatique non amorçable, que cela soit dû à une erreur humaine, à une défaillance matérielle ou logicielle, à une catastrophe naturelle, etc. Dans ces situations, il est fréquent que la partition d'amorçage ou la partition système de l'ordinateur ne soit plus disponible. Il faut alors procéder à une récupération de l'environnement avant de pouvoir commencer l'opération de restauration standard. Le processus de récupération consiste à repartitionner et à reformater la partition d'amorçage, puis à récupérer le système d'exploitation avec toutes les données de configuration qui définissent l'environnement. *Cette étape doit être accomplie pour pouvoir récupérer les autres données utilisateur.*

En règle générale, après la survenue d'un sinistre, le système (appelé **système cible**) est non amorçable et la fonction de récupération après sinistre de Data Protector vise à restaurer la configuration initiale de ce système. La différence entre le système endommagé et le système cible réside dans le fait que, pour le système cible, le matériel défaillant a été remplacé.

Un sinistre est toujours un événement grave, toutefois les facteurs suivants sont susceptibles d'aggraver encore la situation

- Le système doit être rétabli à l'état en ligne aussi vite et efficacement que possible.
- Les administrateurs ne sont pas coutumiers de la procédure requise pour réaliser la récupération après sinistre.

- Il se peut également que le personnel chargé d'effectuer la récupération ne possède qu'une connaissance générale du système.

La récupération après sinistre est une tâche complexe nécessitant une planification et une préparation approfondies avant d'être exécutée. Pour être en mesure de faire face à un sinistre et d'y remédier, un processus détaillé et bien défini doit être en place.

Le **processus de récupération après sinistre** est constitué de quatre phases :

1. La **phase 0** (planification / préparation) est une étape indispensable pour la réussite de la récupération après sinistre.

---

△ **ATTENTION :**

Il est trop tard pour préparer une récupération après sinistre une fois que le sinistre s'est produit.

---

2. Dans la **phase 1**, le DR OS est installé et configuré, ce qui implique généralement un repartitionnement et un reformatage de la partition d'amorçage; en effet, la partition système ou d'amorçage du système n'est pas toujours disponible. Or, l'environnement doit être rétabli avant de pouvoir poursuivre les opérations normales de restauration.
3. Dans la **phase 2**, le système d'exploitation tel qu'il était, c'est-à-dire avec toutes les informations de configuration définissant l'environnement avec Data Protector est restauré.
4. Ce n'est qu'après cette étape que la restauration des applications et des données utilisateur est possible (**phase 3**). Pour que la restauration soit aussi rapide et efficace que possible, il convient d'appliquer un processus en plusieurs étapes bien défini.

## Méthodes de récupération après sinistre

Data Protector prend en charge les méthodes de récupération après sinistre suivantes :

- Récupération après sinistre manuelle  
Méthode de récupération après sinistre de base très souple. Vous devez installer et configurer le DR OS. Ensuite, utilisez Data Protector pour restaurer les données (y compris les fichiers du système d'exploitation) en remplaçant les fichiers du système d'exploitation par ceux du système d'exploitation restauré.
- Récupération après sinistre automatique



La Récupération automatique du système (ASR) est un système automatisé sur les systèmes Windows, qui reconfigure un disque et rétablit son état initial (ou redimensionne les partitions si le nouveau disque est plus grand que le disque initial) dans le cas d'un sinistre. Grâce à la procédure ASR, la commande `drstart.exe` de Data Protector peut ainsi installer le DR OS actif qui fournit à Data Protector l'accès aux disques, au réseau, aux bandes et au système de fichiers.

- Récupération après sinistre avec restitution de disque  
Sur les clients Windows, le disque du système endommagé (ou le disque de rechange pour le disque endommagé physiquement) est temporairement connecté à un système hôte. Une fois la restauration effectuée, le disque peut être reconnecté au système en panne et être amorcé. Sur les systèmes UNIX, le disque auxiliaire, disposant d'un système d'exploitation minimal avec gestion du réseau et sur lequel un Agent de disque Data Protector est installé, est utilisé pour réaliser la récupération après sinistre avec restitution de disque.
- Récupération après sinistre automatique avancée (EADR)  
La fonction Récupération après sinistre automatique avancée (Enhanced Automated Disaster Recovery - EADR) constitue une méthode de récupération Data Protector entièrement automatisée pour les clients Windows et le Gestionnaire de cellule, où l'intervention de l'utilisateur est réduite au minimum. Le système redémarre à partir de l'image ISO du CD de récupération après sinistre, puis Data Protector installe et configure automatiquement le DR OS, formate et partitionne les disques, et enfin rétablit le système d'origine à l'aide de Data Protector, tel qu'il était au moment de la sauvegarde.
- La fonction One Button Disaster Recovery (OBDR) constitue une méthode de récupération Data Protector entièrement automatisée pour les clients Windows et le Gestionnaire de cellule, où l'intervention de l'utilisateur est réduite au minimum. Le système redémarre à partir de la bande OBDR et est automatiquement récupéré.

Pour obtenir la liste des méthodes de récupération après sinistre prises en charge par un système d'exploitation spécifique, consultez les dernières matrices de support à l'adresse <http://www.hp.com/support/manuals>.

## Autres méthodes de récupération après sinistre

Cette section compare le concept de récupération après sinistre de Data Protector avec les solutions proposées par d'autres fournisseurs. Cette section décrit les aspects les plus importants des méthodes de récupération après sinistre alternatives. Deux autres méthodes de récupération sont étudiées :

## Méthodes de récupération après sinistre prises en charge par les fournisseurs de systèmes d'exploitation

La plupart des fournisseurs ont leurs propres méthodes, mais pour ce qui est de la restauration des données, la procédure consiste généralement à effectuer les étapes suivantes :

1. Réinstaller entièrement le système d'exploitation
2. Réinstaller les applications
3. Restaurer les données d'application

Une personnalisation et une reconfiguration manuelles excessives du système d'exploitation et des applications sont nécessaires pour ramener le système à l'état dans lequel il se trouvait avant le sinistre. Ce processus est très complexe et lent, comporte un risque d'erreur important et implique l'utilisation d'outils qui ne sont pas intégrés les uns aux autres. Il ne bénéficie pas de l'avantage que représente une sauvegarde du système d'exploitation, des applications et de leurs configurations dans leur ensemble.

### Récupération avec des outils tiers (pour Windows)

Cette méthode consiste généralement à utiliser un outil spécial permettant de sauvegarder la partition système sous la forme d'un snapshot qui peut ensuite être restauré rapidement. Pour cela, vous devez :

1. Restaurer la partition système (à l'aide de l'outil tiers).
2. Restaurer les autres partitions (qui peuvent être sélectives), le cas échéant, à l'aide de l'outil de sauvegarde standard.

Il apparaît donc clairement que cette méthode implique l'utilisation de deux sauvegardes différentes avec des outils différents. Il s'agit généralement d'une tâche difficile à accomplir. Si vous mettez en œuvre cette méthode dans une grande société, la surcharge administrative liée à la gestion des différentes versions des données (sauvegardes hebdomadaires) avec deux outils différents doit être prise en compte.

Data Protector, pour sa part, représente une solution d'entreprise puissante, complète et polyvalente (inter plates-formes) permettant une récupération après sinistre rapide et efficace, qui inclut la sauvegarde et la restauration et prend en charge la gestion des clusters. Elle offre une administration centralisée et des fonctions de restauration simples, une prise en charge haute disponibilité, des fonctions de contrôle, de génération de rapports et de notification qui soulagent fortement l'administration des systèmes dans le cadre d'une grande entreprise.

---

# 3 Gestion des supports et périphériques

## Dans ce chapitre

Ce chapitre décrit les concepts Data Protector de gestion des supports et périphériques. Les sujets suivants y sont abordés : pools de supports, périphériques et grandes bibliothèques.

Il s'organise comme suit :

“Gestion des supports” à la page 147

“Cycle de vie des supports” à la page 149

“Pools de supports” à la page 150

“Gestion des supports avant le début des sauvegardes” à la page 160

“Gestion des supports pendant une session de sauvegarde” à la page 162

“Gestion des supports après une session de sauvegarde” à la page 167

“Périphériques” à la page 170

“Périphériques autonomes” à la page 178

“Petits périphériques de magasin” à la page 179

“Grandes bibliothèques” à la page 179

“Data Protector et réseaux SAN” à la page 189

## Gestion des supports

La gestion de nombreux supports au niveau de l'entreprise peut s'avérer extrêmement complexe. La fonctionnalité de gestion des supports de Data Protector permet d'allouer des données de sauvegarde à un support de façon souple et efficace. Il est possible

d'utiliser différentes méthodes : l'allocation automatique ou l'allocation stricte de supports.

## Fonctionnalité de gestion des supports

Data Protector fournit les fonctions de gestion des supports décrites ci-après, pour une gestion simple et efficace d'un nombre important de supports :

- Supports regroupés en unités logiques appelées pools de supports : permet de travailler sur de grands groupes de supports, ce qui évite de gérer chacun des supports de façon individuelle.
- Data Protector assure le suivi de tous les supports et enregistre : l'état de chacun d'eux, le délai d'expiration de la protection des données, la disponibilité des supports pour les sauvegardes, ainsi qu'un catalogue des sauvegardes effectuées sur chaque support.
- Possibilité de transférer toutes les données de catalogue relatives au périphérique d'un Gestionnaire de cellule Data Protector à un autre, sans qu'il soit nécessaire d'accéder physiquement aux supports.
- Stratégies de rotation automatisée des supports : évite de devoir gérer manuellement la rotation des bandes.
- Possibilité de définir explicitement les supports et les périphériques à utiliser pour la sauvegarde.
- Gestion des supports optimisée pour des types de périphériques déterminés, tels que les périphériques autonomes, de magasin et de bibliothèque, ainsi que les grands périphériques silo.
- Fonctionnement entièrement automatisé. Si le nombre de supports auxquels Data Protector peut accéder au niveau des périphériques de bibliothèque est suffisamment élevé, la fonctionnalité de gestion des supports permet d'exécuter des sauvegardes pendant des semaines sans intervention d'un opérateur pour s'occuper des supports.
- Reconnaissance et prise en charge des codes-barres assurées sur les périphériques silo et sur certaines grandes bibliothèques.
- Fonction de reconnaissance automatique des formats de support Data Protector et des autres formats de bande courants.
- Data Protector ne permet d'écrire que sur des supports vierges qui ont été initialisés (formatés) dans Data Protector. Data Protector ne peut pas être utilisé pour écraser des formats de bande externes lors d'une sauvegarde, cette restriction permettant d'éviter d'écraser par erreur des supports créés dans d'autres applications.
- Reconnaissance, suivi, affichage et gestion des supports utilisés par Data Protector et séparation de ces supports de ceux utilisés par d'autres applications au niveau des périphériques de bibliothèque et silo.

- Conservation dans un emplacement central des informations sur les supports utilisés et partage de ces informations entre plusieurs cellules Data Protector.
- Prise en charge de la mise au coffre des supports.
- Création interactive ou automatisée de copies supplémentaires des données sur les supports.

Ce chapitre décrit plus en détails la fonctionnalité ci-dessus.

## Cycle de vie des supports

Le cycle de vie caractéristique des supports est composé des phases suivantes :

### 1. Préparation des supports pour la sauvegarde.

Cette phase comporte l'initialisation (formatage) des supports en vue de les utiliser dans Data Protector et leur affectation à des pools de supports, ceux-ci permettant d'effectuer un suivi des supports.

Pour plus de détails, reportez-vous à la section "[Gestion des supports avant le début des sauvegardes](#)" à la page 160.

### 2. Utilisation des supports pour la sauvegarde.

Lors de cette phase, on détermine le mode de sélection des supports pour la sauvegarde, le mode de vérification de l'état des supports et le mode d'ajout de sauvegardes aux supports ; on détermine également à quel stade les données des supports doivent être écrasées.

Pour plus de détails, reportez-vous à la section "[Gestion des supports pendant une session de sauvegarde](#)" à la page 162.

### 3. Mise au coffre des supports pour stockage des données à long terme. Vous pouvez utiliser l'une des méthodes de duplication de données de Data Protector pour réaliser des copies des données sauvegardées à des fins de mise au coffre.

Pour plus de détails sur la mise au coffre, reportez-vous à la section "[Gestion des supports après une session de sauvegarde](#)" à la page 167.

### 4. Recyclage des supports pour de nouvelles sauvegardes une fois que les données contenues sur les supports ne sont plus nécessaires.

### 5. Mise hors service des supports.

Lorsqu'un support est arrivé à expiration, il se voit attribuer l'état "médiocre" et n'est plus utilisé par Data Protector.

Reportez-vous à la section "[Détermination de l'état des supports](#)" à la page 166.

# Pools de supports

Les pools de supports Data Protector permettent de gérer de grandes quantités de supports, réduisant ainsi au minimum le travail de gestion des administrateurs.

## Qu'est-ce qu'un pool de supports ?

Un pool est un ensemble logique de supports partageant les mêmes critères d'utilisation et les mêmes propriétés. Tous les supports d'un pool doivent être du même type physique. Par exemple, des supports DLT et DAT/DDS ne peuvent pas figurer dans un même pool.

L'appartenance d'un support à un pool n'est pas conditionnée par l'emplacement courant de ce support. Il importe peu que le support se situe dans un lecteur, à un emplacement référentiel d'une bibliothèque, dans le coffre ou ailleurs ; il appartient à son pool jusqu'à ce qu'il soit recyclé et exporté de la cellule.

Plusieurs périphériques peuvent utiliser des supports du même pool.

## Exemples de propriétés de pool de supports

Exemples de propriétés de pools :

- ajout possible  
Permet à Data Protector d'ajouter des données aux supports de ce pool lors des sessions de sauvegarde ultérieures.  
Si cette option est désactivée, les supports ne contiendront que des données d'une même session.
- ajout possible aux incrémentales uniquement  
Une session de sauvegarde n'est ajoutée à un support qu'en cas de sauvegarde incrémentale. Cette propriété permet de disposer d'un jeu complet de sauvegardes complètes et incrémentales sur le même support, dans la mesure où l'espace est suffisant.
- stratégie d'allocation de supports  
Il existe plusieurs niveaux de rigueur concernant le choix des supports pour la sauvegarde. Ils vont de strict (Data Protector requiert un support spécifique) à souple (Data Protector accepte tout support adéquat dans le pool, y compris les nouveaux supports).

Chaque périphérique est lié à un pool de supports par défaut. Ce pool peut être modifié au niveau des spécifications de sauvegarde.

Pour plus d'informations sur les autres propriétés des pools de supports, recherchez l'entrée suivante dans l'index de l'aide en ligne : "pool de supports, propriétés".

## Pools de supports et répertoires `dcbf`

Data Protector vous permet de définir un répertoire cible `dcbf` pour un pool de supports. Cela signifie que les informations sur chacun des supports du pool sont stockées dans le répertoire `dcbf` spécifié.

Pour obtenir des informations sur la partie DCBF de la base de données IDB et sur les répertoires `dcbf`, reportez-vous à la section "[Architecture de la base de données IDB](#)" à la page 207.

## Utilisation des pools de supports

L'utilisation des pools dépend essentiellement de vos préférences. Par exemple, les pools peuvent être définis selon les critères suivants :

- plate-forme système (un pool pour les systèmes UNIX, un autre pour les systèmes Windows Vista et un autre pour les systèmes Windows XP)
- par système (chaque système a son propre pool)
- structure organisationnelle (tous les systèmes du service\_A ont un pool et ceux du service\_B un autre)
- catégories de systèmes (grandes bases de données ou applications stratégiques)
- type de sauvegarde (toutes les sauvegardes complètes utilisent un pool et toutes les sauvegardes incrémentales un autre)
- combinaison des critères exposés ci-dessus, etc.

Pour bien comprendre le fonctionnement du système, considérez les pools de supports comme la destination des sauvegardes et les périphériques comme le mécanisme de transfert des données vers les pools de supports.

Pour définir la relation entre un pool et une catégorie de systèmes, il faut associer les mêmes spécifications de sauvegarde à certains systèmes et définir le ou les pools. Les options sélectionnées (lors de la définition des périphériques, des pools et des spécifications de sauvegarde) déterminent le mode d'enregistrement des données des objets sur le support.

Le regroupement de ces supports utilisés pour un même type de sauvegarde en pools permet d'appliquer des stratégies de traitement de supports communes au niveau d'un groupe, ce qui dispense l'utilisateur de traiter chaque support de façon individuelle. Tous les supports d'un pool sont suivis sous forme d'ensemble et partagent une stratégie d'allocation de supports commune.

## Pools de supports par défaut

Data Protector fournit des pools de supports par défaut pour différents types de supports. Ces pools par défaut vous permettent d'exécuter rapidement des sauvegardes sans avoir à créer vos propres pools de supports. Toutefois, dans le cas d'un environnement de grande envergure, il est nécessaire de créer différents pools de supports en fonction des besoins, pour une efficacité maximale. Lorsque vous exécutez une sauvegarde, précisez quel pool de supports vous souhaitez utiliser.

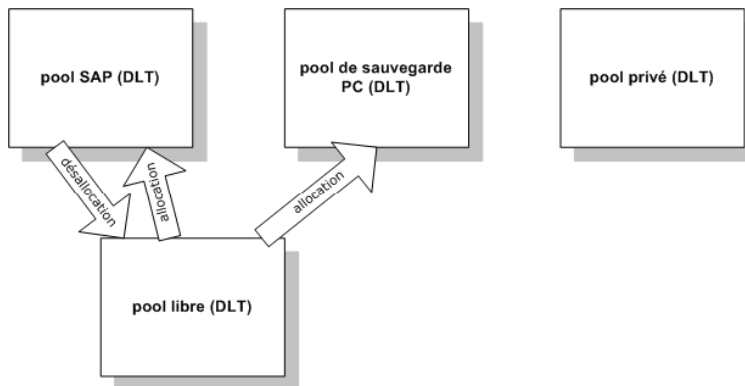
## Pools libres

Si des supports alloués à un pool de supports spécifique sont déjà tous utilisés, vous ne pouvez pas les utiliser dans un autre pool, même si les supports sont du même type. Cette restriction risque d'entraîner inutilement des demandes de montage et l'intervention d'un opérateur. Pour résoudre ce problème, vous pouvez utiliser le modèle de pool unique, selon lequel tous les supports figurent dans le même pool. Bien que cette solution permette de partager les supports libres, elle réduit les avantages liés aux pools de supports, notamment : gestion des données facilitée, séparation des données selon leur degré d'importance, etc. L'utilisation de pools libres permet de pallier cet inconvénient.

## Qu'est-ce qu'un pool libre ?

Un pool libre est une source auxiliaire de supports du même type (DLT, par exemple) utilisée lorsque tous les supports libres d'un pool classique sont épuisés. Il permet d'éviter qu'une sauvegarde échoue en raison d'un manque de supports (libres).





**Figure 38 Pools libres**

### Quand utilise-t-on un pool libre ?

Les supports sont déplacés entre les pools ordinaires et libres dans deux cas (Figure 38 à la page 153) :

- L'allocation. Les supports sont déplacés d'un pool libre vers un pool ordinaire.
- La désallocation. Les supports sont déplacés d'un pool ordinaire vers un pool libre. Vous pouvez configurer le système pour que la désallocation s'exécute automatiquement. Par exemple, les supports du pool de sauvegarde PC illustré à la Figure 38 à la page 153 ne sont pas automatiquement désalloués.

Les supports protégés (alloués, utilisés) appartiennent à un pool ordinaire spécifique (comme le pool SAP), alors que les supports Data Protector libres peuvent être déplacés (automatiquement) vers un pool libre. Ce dernier est ensuite utilisé pour l'allocation de supports libres à tous les pools dont la configuration permet l'utilisation de ce pool libre.

Certains pools classiques, par exemple le pool privé illustré à la Figure 38 à la page 153, peuvent également être configurés pour ne pas partager de supports avec les pools libres.

### Avantages d'un pool libre

Un pool libre présente les avantages suivants :

- Partage des supports libres entre les pools.  
Tous les supports libres (non protégés, vides) peuvent être regroupés dans un pool libre et partagés entre tous les pools de supports prenant en charge l'utilisation des pools libres.
- L'intervention de l'opérateur est limitée dans le cadre de la sauvegarde.

En supposant que tous les supports libres soient partagés, le nombre de demandes de montage nécessaires est réduit.

## Propriétés des pools libres

Un pool libre :

- peut être créé manuellement ou automatiquement lorsque vous configurez son utilisation (il est impossible de supprimer des pools libres s'ils sont liés à un pool ordinaire ou s'ils ne sont pas vides) ;
- est différent d'un pool ordinaire dans le sens où il ne propose pas d'options de stratégie d'allocation ;
- ne contient que des supports Data Protector (supports inconnus ou vierges exclus).

## Détermination de la qualité des supports

La qualité des supports est déterminée sur une base d'égalité entre les pools. Cela signifie que les facteurs d'état d'un support seront configurables pour un pool libre uniquement et que tous les pools utilisant ce pool libre en hériteront.

## Limites des pools libres

Les limites des pools libres sont les suivantes :

- Vous ne pouvez pas sélectionner différents facteurs d'état pour chaque pool. En revanche, tous les pools utilisant un pool libre utilisent les facteurs d'état configurés pour ce pool libre.
- Un support protégé ne peut pas être déplacé vers un pool libre. De même, un support non protégé ne peut pas être déplacé vers un pool ordinaire si la désallocation automatique est activée sur ce pool.
- Vous ne pouvez pas utiliser d'opérations telles que l'importation, la copie et le recyclage sur des supports d'un pool libre.
- Les pools avec prise en charge de magasins ne peuvent pas utiliser de pool libre.
- Certaines incohérences provisoires peuvent apparaître dans les pools en cas d'utilisation de pools libres, par exemple lorsqu'un support non protégé situé dans un pool ordinaire attend le processus de désallocation.
- Si vous changez la protection des supports après son expiration (par exemple en Permanent), même si les supports se trouvent dans un pool libre, ils ne seront pas alloués pour la sauvegarde.
- Lorsqu'ils sont alloués à partir d'un pool libre, des supports avec différents types de formats de données peuvent être utilisés et sont automatiquement reformatés, par exemple les supports NDMP sont reformatés au format normal.

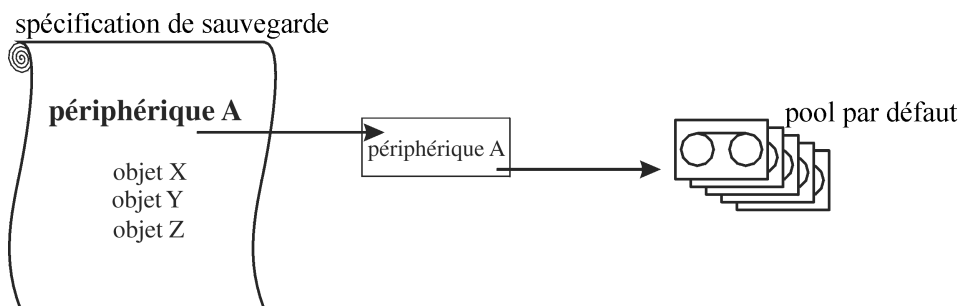
Pour plus d'informations sur les pools libres, recherchez l'entrée suivante dans l'index de l'aide en ligne de Data Protector : "pools libres, caractéristiques".

## Pools de supports, exemples d'utilisation

Les exemples ci-dessous présentent certaines configurations que vous pouvez étudier pour vous aider à choisir la stratégie adéquate en fonction d'un environnement de sauvegarde particulier.

### Exemple 1

Dans le modèle proposé dans la [Figure 39](#) à la page 155, tous les objets sont sauvegardés sur le même pool de supports. La spécification de sauvegarde ne fait référence à aucun pool, c'est la raison pour laquelle le pool par défaut, qui fait partie de la définition du périphérique, est utilisé.

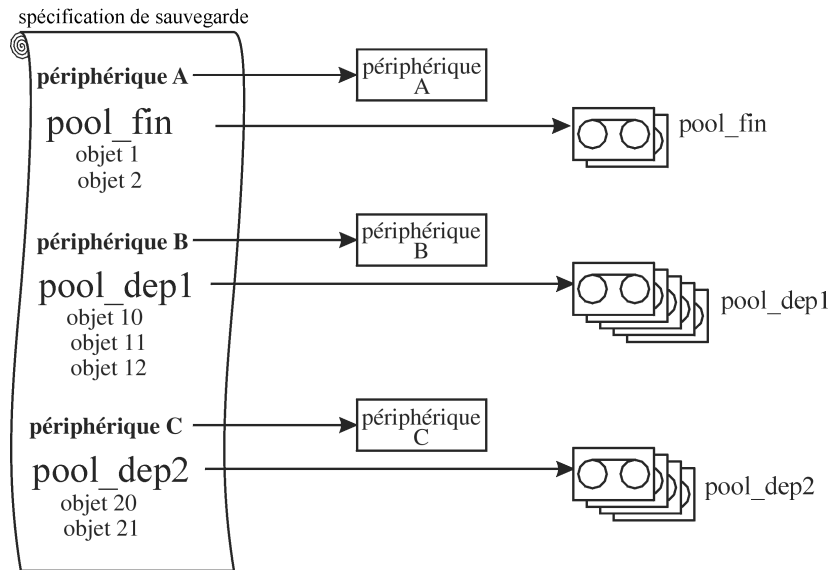


**Figure 39** Relation simple entre un périphérique et un pool de supports

### Exemple 2

Les grands périphériques de bibliothèque contiennent un certain nombre de lecteurs et de supports utilisés par différents services et applications. Vous pouvez configurer un pool de supports pour chaque service, comme le montre la [Figure 40](#) à la page 156, et choisir le lecteur dans la bibliothèque qui effectuera le transfert de données réel. La flèche qui relie une spécification de sauvegarde à un pool de supports indique que vous avez défini un pool de supports cible dans une spécification de sauvegarde. Si vous ne précisez pas de pool de supports dans la spécification de sauvegarde, le pool par défaut, spécifié dans la définition du périphérique, est utilisé.

Pour obtenir plus d'informations sur la relation entre les pools de supports et les grands périphériques de bibliothèque, reportez-vous à la section "[Grandes bibliothèques](#)" à la page 179.

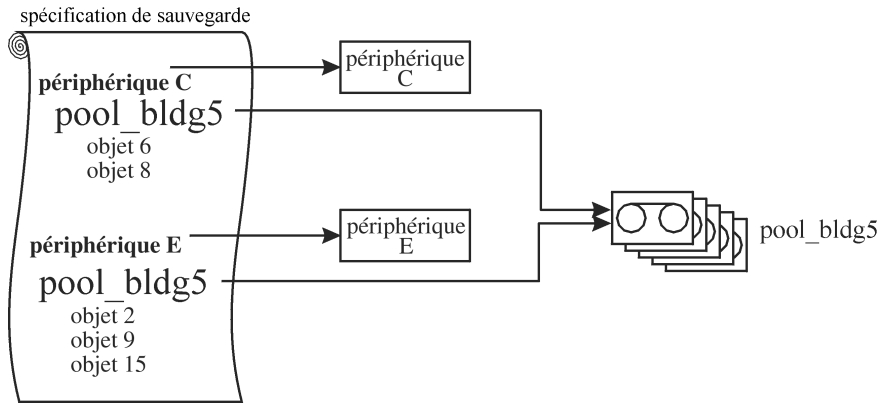


**Figure 40 Configuration des pools de supports pour les grandes bibliothèques**

### Exemple 3

Dans l'exemple présenté à la [Figure 41](#) à la page 157, plusieurs périphériques sont utilisés simultanément pour sauvegarder des données sur des supports d'un pool. Les performances sont améliorées grâce à l'utilisation de plusieurs périphériques en parallèle, quel que soit le pool utilisé.

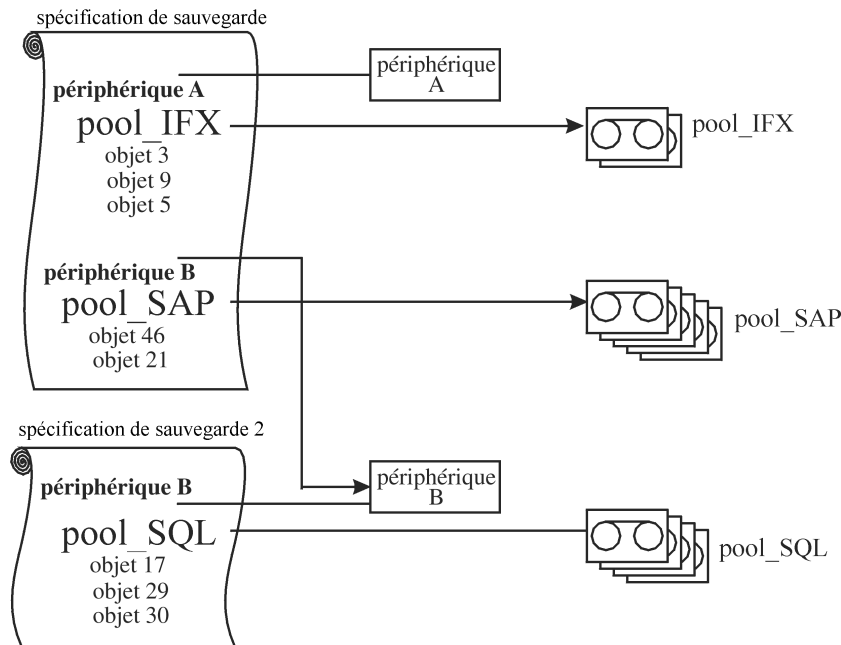
Pour plus de détails, reportez-vous à la section "[Listes de périphériques et partage de charge](#)" à la page 172.



**Figure 41 Périphériques multiples, pool de supports unique**

#### Exemple 4

Plusieurs périphériques sont utilisés simultanément pour sauvegarder des données sur des supports de plusieurs pools. Si vous voulez utiliser le même périphérique avec différents pools, vous devez créer plusieurs spécifications de sauvegarde. Dans l'exemple ci-dessous, un pool de supports séparé est prévu pour chaque application de base de données.



**Figure 42 Périphériques multiples, pools de supports multiples**

## Mise en œuvre d'une stratégie de rotation des supports

### Qu'est-ce qu'une stratégie de rotation des supports ?

Une stratégie de rotation des supports définit le mode d'utilisation des supports lors de la sauvegarde et concerne notamment les points définis ci-après. Pour définir une stratégie de rotation des supports, répondez aux questions suivantes :

- Combien de générations de sauvegarde sont requises ?
- Où sont stockés les supports ?
- A quelle fréquence sont utilisés les supports ?
- Quand les supports peuvent-ils être écrasés et réutilisés pour de nouvelles sauvegardes ?
- Combien de temps les supports peuvent-ils être utilisés avant d'être remplacés ?

Les stratégies de sauvegarde traditionnelles utilisées avec les anciens outils de sauvegarde nécessitaient une stratégie de rotation des supports bien définie et planifiée, contrôlée par l'administrateur plutôt que par l'application de sauvegarde. Data Protector vous permet de mettre en œuvre une stratégie de rotation en spécifiant

les options d'utilisation afin que la sélection des supports pour les sauvegardes ultérieures s'effectue automatiquement.

## Rotation des supports et Data Protector

### Rotation et gestion automatiques des supports

Data Protector automatise la rotation et la gestion des supports de la manière suivante :

- Les supports étant regroupés dans des pools, vous n'avez plus à gérer de supports isolés. Data Protector gère et effectue le suivi de chacun des supports des différents pools.
- Il n'est pas nécessaire de sélectionner les supports sur lesquels les données seront enregistrées ; Data Protector effectue automatiquement cette sélection. Les données sont sauvegardées sur un pool de supports.
- Data Protector sélectionne automatiquement les supports d'un pool en fonction de la stratégie d'allocation des supports et des options d'utilisation que vous avez choisies. Vous pouvez également désactiver la sélection automatique et utiliser la sélection manuelle des supports.
- L'emplacement des supports configurés dans Data Protector est enregistré et indiqué au niveau de l'interface utilisateur Data Protector.
- Data Protector effectue un suivi du nombre d'écrasements effectués sur les supports et de l'âge des supports, ce qui lui permet de définir l'état des supports.
- Data Protector comporte un mécanisme de sécurité permettant d'éviter tout écrasement accidentel des supports contenant des données protégées.

### Supports requis pour la rotation

#### Estimation de la quantité de supports requis

Les étapes suivantes vous aideront à estimer la quantité de supports nécessaires pour une rotation complète :

- Déterminez si les supports disponibles peuvent être utilisés intégralement, ou bien si certains supports ont la propriété Sans possibilité d'ajout et ne peuvent être utilisés que partiellement.
- Déterminez quels systèmes seront sauvegardés, ainsi que l'espace requis sur les supports pour la sauvegarde des données associées. Vous pouvez par exemple utiliser le test de sauvegarde.
- Déterminez la fréquence de sauvegarde, par exemple le nombre de sauvegardes incrémentales à effectuer entre deux sauvegardes complètes.

- Déterminez le nombre de supports requis pour une génération de sauvegarde (une génération de sauvegarde étant constituée d'une sauvegarde complète et de toutes les sauvegardes incrémentales effectuées jusqu'à la sauvegarde complète suivante). Prenez également en compte la compression matérielle si vous avez prévu de l'utiliser avec les périphériques.
- Déterminez la durée pendant laquelle les supports seront protégés.
- Calculez le nombre de générations de sauvegarde qui pourront être créées avant que la première génération de sauvegarde ne soit écrasée.

Vous devriez désormais être capable d'estimer la quantité de supports requis pour une rotation de supports complète. Il vous faudra peut-être prévoir des supports supplémentaires dans la mesure où :

- Data Protector utilise 10 % de l'espace disponible sur les supports pour les données relatives aux répertoires et aux fichiers. La taille indiquée lors du test de sauvegarde comprend ces 10 %.
- Les supports ne satisfont plus les critères d'utilisation ; ils devront alors être remplacés.
- Le volume de données que vous prévoyez de sauvegarder risque d'augmenter.

## Gestion des supports avant le début des sauvegardes

Vous devez initialiser ou formater les supports avant de pouvoir les utiliser pour la sauvegarde dans Data Protector. Vous pouvez les initialiser (formater) manuellement ou laisser Data Protector les initialiser (formater) automatiquement lorsqu'ils sont sélectionnés pour la sauvegarde. Reportez-vous à la section "[Sélection des supports utilisés pour la sauvegarde](#)" à la page 163.

### Initialisation ou formatage des supports

#### Qu'est-ce que l'initialisation (le formatage) des supports ?

Avant d'utiliser les supports pour la sauvegarde, Data Protector les initialise (formate). Les informations relatives à chaque support (ID, description et emplacement) sont enregistrées dans la base de données IDB et écrites sur le support même (en en-tête). Lorsque vous initialisez (formatez) des supports, vous devez également préciser à quel pool de supports ils appartiennent.

Si les supports ne sont pas initialisés (formatés) avant la sauvegarde, Data Protector peut initialiser (formater) des supports vierges au cours de cette sauvegarde en utilisant des étiquettes par défaut, si la définition de la stratégie de pool le permet. La première sauvegarde sur ces supports prendra alors plus de temps. Pour plus de détails,



reportez-vous à la section “[Sélection des supports utilisés pour la sauvegarde](#)” à la page 163.

## Etiquetage des supports Data Protector

### Comment les supports sont-ils étiquetés dans Data Protector ?

Lorsque vous initialisez (formatez) des supports pour les utiliser dans Data Protector, vous devez définir une étiquette qui vous aidera à les identifier par la suite. Si le périphérique dispose d'un lecteur de code-barres, le code-barres est automatiquement affiché comme introduction à la description du support. Le code-barres fournit un ID unique à chaque support dans la base de données IDB. Le cas échéant, vous pouvez utiliser le code-barres comme étiquette du support pendant l'initialisation du support.

Data Protector attribue un ID de support à chaque support, de façon à l'identifier de manière exclusive.

Une étiquette ANSI X3.27 est également inscrite sur la bande, de sorte que celle-ci puisse être identifiée sur d'autres systèmes. Cette étiquette et d'autres informations complémentaires sont inscrites par Data Protector en en-tête des supports et dans la base de données IDB.

Si vous modifiez l'étiquette du support, Data Protector modifie l'étiquette du support dans la base de données IDB et non sur le support lui-même. Par conséquent, si vous exportez et importez des supports n'ayant pas été mis à jour, l'étiquette de la base de données IDB est remplacée par l'étiquette du support. L'étiquette apposée sur la bande ne peut être modifiée qu'en réinitialisant (formatant) le support.

### Comment sont utilisées les étiquettes ?

Les étiquettes identifient le support en tant que support Data Protector. Lors du chargement d'un support pour la sauvegarde ou la restauration, Data Protector consulte l'ID du support. Comme le système de gestion des supports conserve les informations relatives au support, Data Protector peut déterminer si l'action demandée est autorisée pour ce support. Par exemple, lorsque vous essayez d'ajouter une nouvelle sauvegarde à un support, le système de gestion des supports vérifie si la protection des données contenues sur ce support est arrivée à expiration. L'étiquette définie par l'utilisateur sert à identifier un support spécifique.

## Champ Emplacement

Les supports de sauvegarde sont généralement stockés à différents emplacements. Par exemple, les sauvegardes doivent être stockées sur site pour que les données

puissent être rapidement restaurées, tandis que les supports contenant une copie des données sauvegardées sont généralement stockés hors site pour des raisons de sécurité.

Un champ Emplacement est disponible dans Data Protector pour chaque support. L'opérateur peut utiliser ce champ à sa convenance. Le champ Emplacement permet de localiser les supports. Exemples de définitions d'emplacement pertinentes : bibliothèque, hors site, coffre\_1, etc.

Le paramètre d'emplacement des supports est également utile si la version d'objet que vous souhaitez restaurer existe sur plusieurs jeux de supports. Vous pouvez définir la priorité d'emplacement des supports qui influencera la sélection du jeu de supports utilisé pour la restauration. Pour plus d'informations sur la sélection des supports utilisés pour la restauration, reportez-vous à la section "[Sélection du jeu de supports](#)" à la page 139.

## Gestion des supports pendant une session de sauvegarde

### Que se passe-t-il pendant la sauvegarde ?

Pendant une session de sauvegarde, Data Protector sélectionne automatiquement les supports et effectue un suivi des données sauvegardées et des supports utilisés. Cela simplifie la gestion des supports, car l'opérateur n'a pas besoin de savoir exactement quelles données ont été sauvegardées, ni quels supports ont été utilisés. Les objets sauvegarde ayant été sauvegardés lors d'une même session constituent un jeu de supports.

Cette section traite des sujets suivants :

- Comment Data Protector sélectionne-t-il les supports qui seront utilisés pour la sauvegarde ?
- Comment les sauvegardes complètes et incrémentales sont-elles ajoutées aux supports ?
- Comment l'état des supports est-il défini ?

Pour obtenir un complément d'informations, consultez les sections suivantes :

- "[Sauvegardes complètes et incrémentales](#)" à la page 72
- "[Pools de supports](#)" à la page 150

## Sélection des supports utilisés pour la sauvegarde

Data Protector sélectionne automatiquement les supports en fonction des stratégies d'allocation des supports. Cela simplifie considérablement la gestion et le traitement des supports étant donné que l'opérateur de sauvegarde n'a pas besoin d'administrer manuellement les supports pour la sauvegarde.

### Stratégie d'allocation de supports

Vous pouvez définir le mode de sélection des supports pour la sauvegarde à l'aide de la stratégie d'allocation des supports. Vous pouvez choisir une stratégie souple, selon laquelle tout support approprié est utilisé pour la sauvegarde, y compris les nouveaux supports et les supports vierges ou une stratégie stricte, selon laquelle les supports doivent être disponibles dans un ordre prédéfini pour faciliter une utilisation équilibrée des supports. Vous pouvez en outre utiliser une liste de préallocation.

### Préallocation de supports

Data Protector vous permet de spécifier explicitement les supports d'un pool à utiliser pour une sauvegarde. Pour ce faire, vous devez avoir recours à une liste de préallocation et combiner celle-ci à une stratégie d'allocation stricte. Les supports sont alors utilisés dans l'ordre spécifié. Si les supports n'apparaissent pas dans cet ordre, Data Protector émet une demande de montage.

### Etat des supports

L'état des supports influe également sur la sélection des supports utilisés pour la sauvegarde. Par exemple, les supports en bon état sont utilisés en priorité par rapport aux supports d'état passable. Pour plus de détails, reportez-vous à la section "[Détermination de l'état des supports](#)" à la page 166.

## Ajout de données aux supports pendant des sessions de sauvegarde

Pour optimiser l'utilisation de l'espace disponible sur les supports et l'efficacité de la sauvegarde et de la restauration, vous pouvez définir la façon dont l'espace laissé sur le support par la sauvegarde précédente sera traité par Data Protector. Cela sera défini dans une stratégie d'utilisation de supports.

### Stratégie d'utilisation de supports

Les stratégies d'utilisation de supports disponibles sont énoncées ci-dessous :

### Ajout possible

Une session de sauvegarde commence à écrire des données dans l'espace restant sur le dernier support utilisé lors d'une précédente session de sauvegarde. L'écriture des données sur les autres supports requis dans le cadre de cette session commence au début de la bande : seules des bandes non protégées ou de nouvelles bandes peuvent donc être utilisées. L'ajout de supports permet d'économiser de l'espace sur les supports mais peut aussi compliquer la mise au coffre car un support peut contenir des données provenant de différents jeux de supports.

### Sans possibilité d'ajout

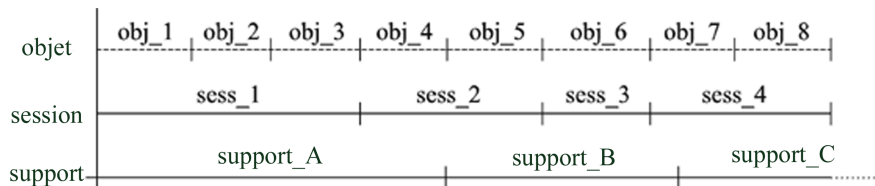
Lors d'une session de sauvegarde, le système commence par écrire les données au début du premier support disponible pour la sauvegarde. Un support ne peut pas contenir de données issues de deux sessions différentes. Cette stratégie simplifie la mise au coffre.

### Ajout possible aux incrémentales uniquement

Une session de sauvegarde n'est ajoutée à un support qu'en cas de sauvegarde incrémentale. Cette propriété permet de disposer d'un jeu complet de sauvegardes complètes et incrémentales sur le même support, dans la mesure où l'espace est suffisant.

## Distribution d'objets sur des supports

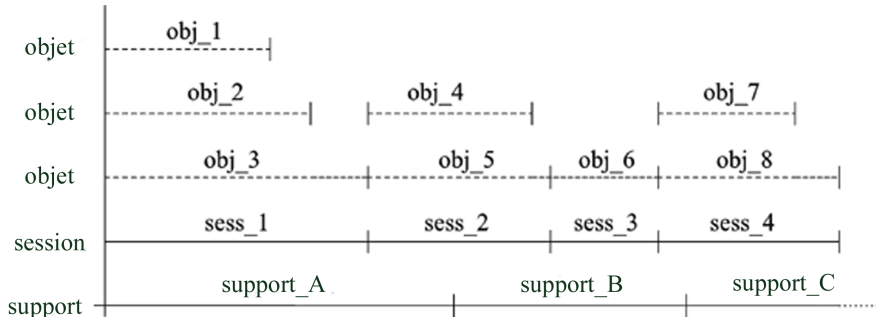
Les figures suivantes présentent quelques exemples de distribution d'objets sur des supports :



**Figure 43 Plusieurs objets et sessions par support, écritures séquentielles**

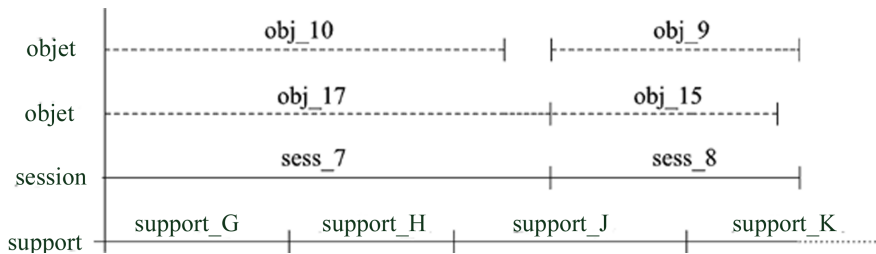
La Figure 43 à la page 164 présente un exemple de huit écritures séquentielles sur quatre sessions, utilisant la stratégie d'utilisation de supports avec ajout possible. Les données ont été écrites en quatre sessions, objet par objet. Les trois supports

appartiennent au même pool de supports. Le *support\_A* et le *support\_B* sont déjà saturés, alors que le *support\_C* dispose encore d'espace.



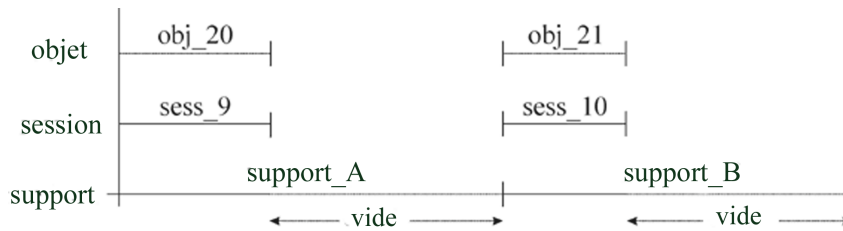
**Figure 44 Plusieurs objets et sessions par support, écritures simultanées**

La Figure 44 à la page 165 présente un exemple de huit objets écrits sur quatre sessions, les paramètres de simultanéité permettant des écritures simultanées. Dans ce cas, les objets *obj\_1*, *obj\_2* et *obj\_3* ont été sauvegardés simultanément lors de la session *sess\_1* ; les objets *obj\_4* et *obj\_5* dans la session *sess\_2*, et ainsi de suite. *Obj\_1* peut provenir de *system\_A* et *obj\_2* de *system\_B*, ou ils peuvent provenir tous deux de différents disques sur le même système. Les ajouts sont possibles dans le cadre de cette stratégie d'utilisation des supports.



**Figure 45 Plusieurs supports par session et par objet**

La Figure 45 à la page 165 présente un exemple de quatre objets sauvegardés ayant été sauvegardés lors de deux sessions, les objets de la première paire ayant été écrits simultanément au cours de *sess\_7* et ceux de la seconde au cours de *sess\_8*. Notez qu'un objet peut s'étendre sur plusieurs supports. Les ajouts sont possibles dans le cadre de cette stratégie d'utilisation des supports.



**Figure 46** Chaque objet est écrit sur un support séparé

Dans l'exemple présenté à la [Figure 46](#) à la page 166, une spécification de sauvegarde est utilisée par objet et la stratégie d'utilisation de supports appliquée est celle sans ajout possible. Le nombre de supports utilisé est supérieur. Si l'on combine cette méthode à la stratégie Ajout possible aux incrémentales uniquement, les sauvegardes incrémentales de l'objet sont écrites sur le même support.

Pour obtenir plus d'informations sur les répercussions des stratégies de sauvegardes complètes et incrémentales sur les performances de la restauration et de l'utilisation des supports, reportez-vous à la section "[Sauvegardes complètes et incrémentales](#)" à la page 72.

## Écriture de données sur plusieurs jeux de supports pendant la sauvegarde

Pendant une session de sauvegarde, vous pouvez écrire simultanément tout ou partie des objets sur plusieurs jeux de supports, à l'aide de la fonction de mise en miroir d'objet de Data Protector. Pour plus de détails, reportez-vous à la section "[Mise en miroir d'objets](#)" à la page 130.

## Détermination de l'état des supports

### Facteurs d'état des supports

Data Protector détermine l'état des supports utilisés à l'aide de **facteurs d'état des supports**. L'état du support le plus médiocre dans un pool détermine l'état de l'ensemble du pool. Par exemple, dès que l'état d'un support dans un pool est médiocre, l'état du pool devient médiocre. Lorsque ce support particulier est supprimé du pool, l'état redevient soit passable, soit bon.

Les supports peuvent présenter trois états : bon, passable ou médiocre.

L'état est défini en fonction des éléments suivants, support par support :

- Nombre d'écrasements

Le degré de vétusté d'un support est déterminé par le nombre d'écrasements réalisés depuis le début de son cycle de vie. Lorsque la limite du nombre d'écrasements définie pour le support est dépassée, il est marqué comme médiocre.

- Age des supports

L'âge d'un support est calculé en fonction du nombre de mois écoulés depuis son formatage ou initialisation. Lorsque la limite du nombre de mois définie pour le support est dépassée, il est marqué comme médiocre.

- Erreurs de périphérique

Le support peut être marqué comme médiocre suite à certaines erreurs de périphérique. Si une erreur se produit au niveau du périphérique pendant une sauvegarde, le support utilisé pour la sauvegarde dans ce périphérique se voit attribuer l'état médiocre.

## Gestion des supports après une session de sauvegarde

Une fois les données écrites sur les supports, vous devez prendre les mesures nécessaires pour protéger les supports et les données qu'ils contiennent. Prenez en compte les points suivants :

- Protection des supports contre les écrasements.

Cette protection a été définie au moment de la configuration de la sauvegarde, mais vous pouvez la modifier après la sauvegarde. Pour plus d'informations sur la protection des données et du catalogue, reportez-vous à la section "[Conservation des données sauvegardées et des informations sur les données](#)" à la page 106.

- Protection des supports contre les dommages physiques.

Les supports contenant des données permanentes peuvent être stockés dans un endroit sûr.

- Copie des données sauvegardées et conservation des copies dans un endroit sûr

Reportez-vous à la section "[Duplication de données sauvegardées](#)" à la page 121.

Les sections suivantes décrivent la manière dont les supports sont mis au coffre et la restauration à partir des supports en question.

## Mise au coffre

### Qu'est-ce que la mise au coffre ?

La mise au coffre est une procédure consistant à stocker en lieu sûr des supports contenant des données importantes ; les supports sont ainsi stockés pendant une période déterminée. Le lieu où sont stockés les supports est généralement appelé **coffre**.

Les fonctions suivantes permettent la mise au coffre dans Data Protector :

- Stratégies de protection des données et du catalogue.
- Sélection et éjection des supports d'une bibliothèque.
- Le champ **Emplacement de supports** indique l'emplacement physique des supports.
- Rapport indiquant les supports utilisés pour la sauvegarde au cours d'une période donnée.
- Rapport indiquant les spécifications de sauvegarde ayant utilisé des supports spécifiques lors de la sauvegarde.
- Rapport sur les supports stockés à un emplacement spécifique avec une protection des données expirant à un moment particulier.
- Présentation de la liste des supports nécessaires à la restauration de données spécifiques et des emplacements physiques où sont stockés ces supports.
- Filtrage des supports affichés selon des critères spécifiques.

### Implémentation de la mise au coffre

L'implémentation de la mise au coffre dépend de la stratégie de sauvegarde adoptée par l'entreprise et de sa stratégie de gestion des données et des supports. Elle comporte généralement les étapes suivantes :

1. Spécification des stratégies de protection des données et de catalogue lors de la configuration des spécifications de sauvegarde.
2. Configuration d'un coffre dans Data Protector. Cela consiste principalement à indiquer le nom du coffre que vous utiliserez pour les supports, par exemple : Coffre\_1.
3. Mise en place de la stratégie de gestion des supports appropriée pour les supports du coffre.



4. En option, création de copies supplémentaires des données sauvegardées à des fins de mise au coffre, utilisation de la fonctionnalité de mise en miroir d'objet pendant la sauvegarde ou de la fonctionnalité de copie d'objet ou de copie de supports après la sauvegarde.
5. Sélection des supports à mettre au coffre, éjection des supports et stockage dans le coffre.
6. Sélection des supports du coffre contenant des données expirées et insertion de ces supports dans une bibliothèque.

### Exemple de mise au coffre

Supposons que la stratégie de sauvegarde de votre entreprise exige que les données soient sauvegardées de façon quotidienne. Chaque semaine, une sauvegarde complète doit être stockée dans un coffre où elle doit rester disponible pendant les cinq années qui suivent. Vous devez être en mesure de restaurer facilement les données de toutes les sauvegardes des années précédentes, stockées dans le coffre. Au bout des cinq années, les supports du coffre peuvent être réutilisés.

Les paramètres suivants de Data Protector doivent être sélectionnés : sauvegarde complète une fois par semaine et sauvegardes incrémentales quotidiennes, protection des données réglée sur cinq ans et protection de catalogue réglée sur un an. Vous pourrez donc simplement explorer et restaurer des données pendant un an et les données resteront disponibles pendant cinq ans pour restauration à partir des supports. Les supports créés lors de la sauvegarde complète sont copiés et stockés dans un coffre. Au bout d'un an, Data Protector supprime automatiquement les informations détaillées de la base de données IDB relatives aux données contenues sur les supports, libérant ainsi de l'espace dans la base de données pour de nouvelles informations.

### Restauration à partir de supports stockés dans un coffre

La restauration des supports stockés dans un coffre est identique à celle réalisée à partir de tout autre support. Selon les stratégies de protection des données et de catalogue que vous aurez choisies, vous devrez éventuellement effectuer quelques étapes supplémentaires :

1. Récupérer les supports stockés dans le coffre et les insérer dans un périphérique.

2. Si la protection de catalogue est toujours valide dans le cas de ces supports, vous pouvez restaurer les données souhaitées en les sélectionnant simplement à l'aide de l'interface utilisateur Data Protector.

Si la protection de catalogue pour les supports est arrivée à expiration, Data Protector ne dispose pas d'informations détaillées sur les données sauvegardées. Vous devez effectuer la restauration en spécifiant manuellement quels fichiers ou répertoires vous souhaitez restaurer. Vous pouvez également restaurer l'objet entier sur un disque de rechange, puis rechercher des fichiers et répertoires dans le système de fichiers restauré.

---

 **CONSEIL :**

Pour obtenir de nouveau les informations détaillées sur les fichiers et répertoires sauvegardés sur les supports après expiration de la protection de catalogue, exportez ces supports puis réimportez-les. Précisez ensuite que vous souhaitez lire les données du catalogue des détails de ces supports. Vous serez de nouveau en mesure de sélectionner des fichiers et des répertoires dans l'interface utilisateur Data Protector.

---

Pour plus d'informations sur la manière dont les stratégies de protection des données et du catalogue influent sur les restaurations, reportez-vous à la section “[Conservation des données sauvegardées et des informations sur les données](#)” à la page 106.

## Périphériques

Data Protector prend en charge un certain nombre de périphériques disponibles sur le marché. La liste actualisée des périphériques pris en charge est accessible à l'adresse <http://www.hp.com/support/manuals>.

### Utilisation des périphériques dans Data Protector

Pour pouvoir utiliser un périphérique dans Data Protector, vous devez le configurer dans la cellule Data Protector. Lorsque vous configurez un périphérique, vous devez lui attribuer un nom, lui associer un pool de supports et définir des options spécifiques, telles que la prise en charge des codes-barres ou des bandes nettoyantes. La procédure de configuration de périphériques est simplifiée par l'assistant qui vous guide tout au long des étapes et qui peut détecter et configurer automatiquement des périphériques. Le même périphérique physique peut être défini plusieurs fois avec différentes propriétés d'utilisation dans Data Protector, par exemple, sans compression de données matérielle dans un cas et avec compression de données matérielle dans

un autre. Pour ce faire, vous devez spécifier des noms de périphérique (logique) différents.

Les sections suivantes décrivent certaines fonctionnalités liées spécifiquement aux périphériques et expliquent le mode de fonctionnement de Data Protector associé à différents périphériques.

### Prise en charge de la console de gestion de bibliothèque

De nombreuses bibliothèques de bandes modernes disposent d'une console de gestion qui permet de configurer, de gérer ou de contrôler les bibliothèques à partir d'un système distant. L'étendue des tâches pouvant être effectuées à distance dépend de l'implémentation de la console de gestion, laquelle est indépendante de Data Protector.

Data Protector simplifie l'accès à l'interface de la console de gestion de bibliothèque. Il est possible de spécifier l'URL (adresse Internet) de la console de gestion pendant le processus de configuration ou de reconfiguration de la bibliothèque. En sélectionnant un élément de menu dédié dans l'interface utilisateur, on appelle un navigateur Web et l'interface de la console est automatiquement chargée.

La liste des types de périphériques pour lesquels cette fonction est disponible est accessible à l'adresse <http://www.hp.com/support/manuals>.

---

#### ❗ IMPORTANT :

Avant d'utiliser la console de gestion de bibliothèque, sachez que certaines opérations effectuées au moyen de la console peuvent interférer avec vos tâches de gestion des supports et/ou vos sessions de sauvegarde et de restauration.

---

### TapeAlert

TapeAlert est un utilitaire de messagerie et de surveillance d'état des périphériques à bandes qui facilite la détection des problèmes pouvant avoir un impact sur la qualité de la sauvegarde. TapeAlert envoie des alarmes ou des messages d'erreur faciles à interpréter au moment où les problèmes surgissent (utilisation de bandes usées, défauts matériels d'un périphérique, etc.), et propose des solutions pour y remédier.

Data Protector prend intégralement en charge TapeAlert 2.0, tant que les périphériques connectés proposent également cette fonctionnalité.

## Listes de périphériques et partage de charge

### Périphériques multiples pour la sauvegarde

Lorsque vous configurez une spécification de sauvegarde, vous pouvez spécifier plusieurs périphériques autonomes ou plusieurs lecteurs dans un périphérique de bibliothèque qui seront utilisés pour cette opération. Cela permet d'accélérer l'opération, les données étant sauvegardées en parallèle sur plusieurs périphériques (lecteurs).

### Équilibrage de l'utilisation des périphériques

Par défaut, Data Protector équilibre automatiquement la charge (l'utilisation) des périphériques afin de les utiliser de manière uniforme. C'est ce qu'on appelle **partage de charge**. Ce procédé permet d'optimiser l'utilisation des périphériques en équilibrant le nombre des objets sauvegardés sur chacun. Cette opération s'effectuant automatiquement pendant la sauvegarde, l'utilisateur n'a pas besoin de gérer l'affectation des objets aux périphériques utilisés au cours de la session ; il lui suffit de spécifier les périphériques à utiliser.

### Quand utiliser le partage de charge ?

Utilisez le partage de charge lorsque :

- Vous sauvegardez un grand nombre d'objets.
- Vous utilisez des périphériques de bibliothèque (changeur automatique) avec plusieurs lecteurs.
- Vous n'avez pas besoin de savoir sur quels supports seront sauvegardés les objets.
- Vous disposez d'une bonne connexion réseau.
- Vous souhaitez augmenter la fiabilité des sauvegardes. En cas d'échec d'un périphérique, Data Protector redirige automatiquement la sauvegarde vers d'autres périphériques sélectionnés à partir d'une liste de périphériques.

### Quand ne pas utiliser le partage de charge ?

N'utilisez pas le partage de charge lorsque :

- Vous voulez sauvegarder un petit nombre d'objets volumineux. Dans ce cas, Data Protector ne peut généralement pas équilibrer la charge entre les périphériques de façon efficace.
- Vous voulez sélectionner les périphériques sur lesquels seront sauvegardés les objets.

## Chaînage de périphériques

Data Protector vous permet de configurer plusieurs périphériques autonomes de même type, connectés au même système, en tant que chaîne de périphériques. 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.

## Fonctionnement du partage de charge

Supposez par exemple que 100 objets soient configurés pour la sauvegarde sur quatre périphériques avec une simultanéité de trois et que les paramètres de partage de charge `MIN` et `MAX` aient chacun la valeur deux. Si au moins deux périphériques sont disponibles, la session démarre avec la sauvegarde de trois objets en parallèle sur les deux premiers périphériques disponibles. Les 94 autres objets sont mis en file d'attente et aucun périphérique ne leur est affecté à ce moment là.

Lorsque la sauvegarde d'un objet est terminée, l'objet suivant dans la file d'attente est affecté au périphérique qui a moins de trois objets simultanément en cours de sauvegarde. Le partage de charge permet de garantir le fonctionnement de deux périphériques en parallèle tant qu'il reste des objets à sauvegarder. Si un périphérique vient à s'interrompre au cours de la sauvegarde, un des deux périphériques en réserve est utilisé. Les objets en cours de sauvegarde sur le périphérique défaillant sont abandonnés, et les trois objets suivants sont affectés au nouveau périphérique. Ainsi, la défaillance d'un périphérique ne peut pas entraîner l'abandon de plus de trois objets, à condition que les autres périphériques soient disponibles pour que la session de sauvegarde continue.

## Périphérique en mode continu et simultanéité

### Qu'est-ce que le fonctionnement en continu d'un périphérique ?

Pour optimiser les performances d'un périphérique, celui-ci doit être alimenté en continu. 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, la bande du support doit être arrêtée pendant que le périphérique attend les données supplémentaires. En d'autres termes, si la vitesse à laquelle les données sont écrites sur la bande est inférieure ou égale à celle à laquelle le système informatique les fournit au périphérique, ce dernier fonctionne en mode continu. Dans des infrastructures de sauvegarde en réseau, cela mérite une attention particulière. Dans le cadre d'une sauvegarde locale, les disques et les périphériques étant reliés au même système, une simultanéité de 1 peut suffire si vos disques sont suffisamment rapides.

## Procédure à suivre pour la configuration d'un périphérique en mode continu

Pour permettre au périphérique de fonctionner en mode continu, une quantité de données suffisante doit lui être envoyée. Pour parvenir à cet objectif, Data Protector démarre plusieurs Agents de disque pour chaque Agent de support écrivant des données sur le périphérique.

### Agents de disque simultanés

La **simultanéité de sauvegarde** des **Agents de disque** correspond au nombre d'Agents de disque lancés pour chaque Agent de support ; ce nombre peut être modifié par le biais des options **avancées** liées au périphérique ou lors de la configuration d'une sauvegarde. Data Protector fournit des valeurs par défaut qui conviennent dans la plupart des cas. Par exemple, pour un périphérique DDS standard, deux Agents de disque envoient suffisamment de données pour que le périphérique fonctionne en mode continu. Si vous utilisez un périphérique de bibliothèque équipé de plusieurs lecteurs et que chaque lecteur est contrôlé par un Agent de support, vous pouvez régler la simultanéité indépendamment pour chaque lecteur.

### Performances accrues

Lorsqu'elle est correctement configurée, la simultanéité de sauvegarde améliore les performances de la sauvegarde. Par exemple, si un périphérique de bibliothèque dispose de quatre lecteurs, chacun étant contrôlé par un Agent de support et chaque Agent de support recevant des données de deux Agents de disque simultanément, les données de huit disques sont sauvegardées simultanément.

Le fonctionnement en mode continu d'un périphérique dépend également d'autres facteurs, tels que la charge du réseau et la taille de bloc des données écrites sur le périphérique.

Pour plus d'informations, reportez-vous à la section "[Sessions de sauvegarde](#)" à la page 239.

### Flux de données multiples

Data Protector permet de sauvegarder simultanément différentes parties d'un disque via plusieurs périphériques. Cette fonction permet de sauvegarder des disques rapides et de grande capacité sur des périphériques relativement lents. Plusieurs Agents de disque lisent les données du disque en parallèle et les envoient à plusieurs Agents de support. Cette méthode accélère la procédure de sauvegarde, à condition de prendre en compte les éléments suivants :

Si un point de montage a été sauvegardé via plusieurs Agents de disque, les données sont contenues dans plusieurs objets. Pour restaurer la totalité du point de montage,

vous devez définir toutes les parties de celui-ci dans une spécification de sauvegarde unique, puis restaurer l'ensemble de la session.

## Taille de segment

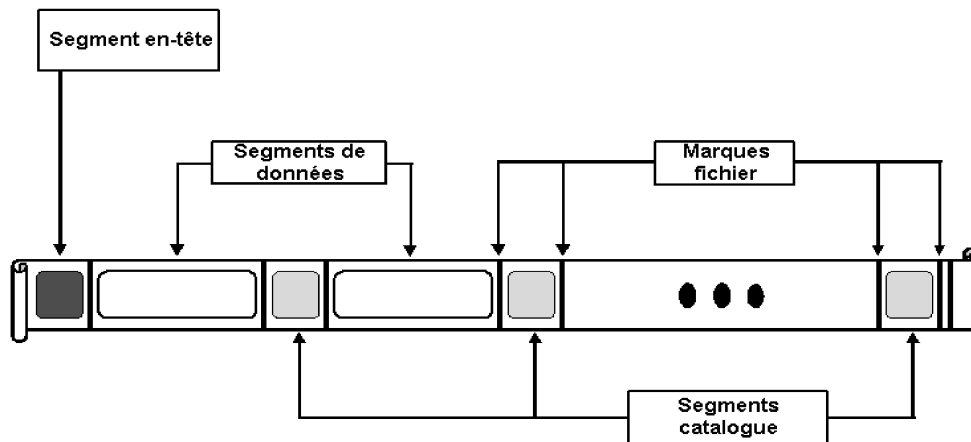
Un support est composé de segments de données, de segments de catalogue et d'un segment d'en-tête. Les informations d'en-tête sont stockées dans le segment d'en-tête, dont la taille est identique à celle du bloc. Les données sont enregistrées dans des blocs de données des segments de données. Les informations concernant chaque segment de données sont stockées dans le segment de catalogue correspondant. Ces informations sont tout d'abord stockées dans la mémoire de l'Agent de support, puis écrites dans un segment de catalogue sur le support, ainsi que dans la base de données IDB. Tous les segments sont séparés par des marques comme le montre la Figure 47 à la page 175.

---

### REMARQUE :

Certaines technologies de bande limitent le nombre de marques de fichier par support. Assurez-vous que la taille de votre segment n'est pas trop réduite.

---



**Figure 47** Format de données

La taille de segment, mesurée en méga-octets, correspond à la taille maximale des segments de données. Si vous sauvegardez un grand nombre de petits fichiers, la taille de segment réelle peut être limitée par la taille maximale des segments de

catalogue. La taille de segment peut être configurée par l'utilisateur pour chaque périphérique. Elle influe sur la rapidité d'une restauration. Une taille de segment réduite limite l'espace disponible sur le support pour les données : en effet, chaque segment dispose d'une marque qui utilise de l'espace sur les supports. Cependant, un grand nombre de marques de fichier permettent d'accélérer les restaurations, un Agent de support pouvant localiser plus rapidement le segment contenant les données à restaurer. La taille de segment optimale dépend du type de support utilisé dans le périphérique et du type de données à sauvegarder. Par exemple, la taille de segment par défaut du support DLT est de 150 Mo.

## Taille de bloc

Les segments ne sont pas écrits en une seule partie mais en plusieurs parties appelées "blocs". Le périphérique traite les données par unités selon une taille de bloc spécifique au type de périphérique. Data Protector permet de régler la taille des blocs envoyés au périphérique. La taille de bloc par défaut pour l'ensemble des périphériques est de 64 Ko.

Vous pouvez améliorer les performances en augmentant la taille de bloc. Vous devez effectuer le changement de taille de bloc *avant* le formatage des bandes. Par exemple, une bande écrite avec la taille de bloc par défaut ne peut pas être complétée avec une taille de bloc différente.



### REMARQUE :

Utilisez la même taille de bloc pour les supports pouvant être utilisés avec différents types de périphériques. Data Protector ne peut ajouter des données qu'aux supports utilisant la même taille de bloc.

---

## Nombre de mémoires tampon utilisées par les Agents de disque

Les Agents de disque et les Agents de support Data Protector utilisent des mémoires tampon pour stocker les données à transférer. La mémoire est divisée en plusieurs zones tampon (une pour chaque Agent de disque, en fonction du nombre de périphériques fonctionnant simultanément). Chaque zone tampon est composée de 8 mémoires tampon d'Agent de disque (de la même taille que celle du bloc configuré pour le périphérique). Vous pouvez remplacer cette valeur par tout nombre compris entre 1 et 32, bien que cela soit rarement nécessaire. Ces paramètres peuvent être changés pour deux raisons principales :

- Mémoire insuffisante



La mémoire partagée requise par un Agent de support peut être calculée de la manière suivante :

$\text{Simultanéité\_AD} * \text{Nombre\_mémoires\_tampon} * \text{Taille\_de\_bloc}$

Si vous réduisez le nombre de mémoires tampon de 8 à 4, par exemple, la consommation de mémoire sera réduite de 50 % et les performances des processus augmenteront.

- Mode continu

Si la bande passante du réseau varie sensiblement au cours de la sauvegarde, il est important que l'Agent de support possède suffisamment de données prêtes à être écrites pour alimenter le périphérique en mode continu. Dans ce cas, augmentez le nombre de mémoires tampon.

## Verrouillage de périphérique et noms de verrouillage

### Noms de périphérique

Lorsque vous configurez des périphériques à l'aide de Data Protector, vous pouvez définir le même périphérique physique plusieurs fois avec des caractéristiques différentes. Pour ce faire, il suffit d'attribuer des noms différents à un même périphérique dans Data Protector. Par exemple, bien que cela ne soit pas recommandé, un périphérique autonome DDS peut être configuré comme périphérique compressé puis non compressé.

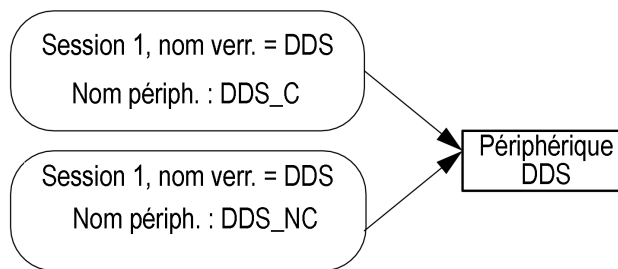
### Conflit de périphériques physiques

Lorsque vous spécifiez un périphérique utilisé pour la sauvegarde, vous pouvez indiquer un nom de périphérique dans une spécification de sauvegarde, et un autre nom pour le même périphérique physique dans une autre spécification de sauvegarde. Selon la planification des sauvegardes, il se peut que Data Protector essaie d'utiliser le même périphérique physique dans le cadre de sessions de sauvegarde différentes, créant ainsi un conflit.

### Prévention des conflits

Afin d'éviter ce type de conflit, spécifiez un nom de verrouillage virtuel dans chaque configuration de périphérique. Data Protector vérifie que les périphériques ont le même nom de verrouillage et évite tout conflit.

Supposons qu'un périphérique autonome DDS ait été configuré comme périphérique compressé sous le nom DDS\_C et comme périphérique non compressé sous le nom DDS\_NC, comme indiqué à la [Figure 48](#) à la page 178. Spécifiez le même nom de verrouillage, DDS, pour les deux périphériques.



**Figure 48 Verrouillage de périphérique et noms de périphérique**

## Périphériques autonomes

### Que sont les périphériques autonomes ?

Les périphériques autonomes sont des périphériques disposant d'un lecteur qui lit/écrit sur un support à la fois.

Les périphériques autonomes sont utilisés pour des sauvegardes à petite échelle ou pour des sauvegardes spéciales. Lorsque le support est saturé, l'opérateur doit le remplacer manuellement par un nouveau support pour que la sauvegarde puisse continuer.

### Data Protector et les périphériques autonomes

Lorsque vous avez relié un périphérique au système, vous devez recourir à l'interface utilisateur Data Protector pour le configurer et pouvoir l'utiliser dans Data Protector. Pour ce faire, vous devez installer un Agent de support Data Protector sur le système auquel le périphérique est connecté. Data Protector peut détecter et configurer automatiquement la plupart des périphériques autonomes.

Pendant une sauvegarde, Data Protector émet une demande de montage lorsque le support d'un périphérique est saturé. L'opérateur doit alors remplacer le support pour que la sauvegarde puisse continuer.

### Que sont les chaînes de périphériques ?

Data Protector vous permet de définir plusieurs périphériques autonomes en tant que chaîne de périphériques. 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.

Les chaînes de périphériques permettent de lancer des sauvegardes sans surveillance axées sur plusieurs périphériques autonomes, évitant ainsi à l'utilisateur de devoir insérer/éjecter manuellement des supports lorsque les supports utilisés sont pleins.

### Périphériques chargeurs

Les périphériques chargeurs, similaires aux chaînes de périphériques, contiennent un certain nombre de supports à utiliser dans un ordre séquentiel. Lorsqu'un support est plein, le support suivant est chargé et utilisé pour la sauvegarde.

## Petits périphériques de magasin

### Que sont les périphériques de magasin ?

Les périphériques de magasin regroupent un certain nombre de supports dans une même unité appelée magasin. Data Protector considère le magasin comme un support unique. Un magasin possède une plus grande capacité qu'un support unique et il est plus facile à gérer que plusieurs supports séparés. La liste des périphériques pris en charge est accessible à l'adresse <http://www.hp.com/support/manuals>.

### Data Protector et les périphériques de magasin

Data Protector vous permet de réaliser des tâches de gestion sur des supports regroupés en magasins, telle que l'émulation d'un support unique via différentes vues de magasins et de supports ou sur un support unique.

Vous pouvez également utiliser un périphérique de magasin en tant que bibliothèque standard, sans tenir compte de la fonction Data Protector de prise en charge des magasins. Data Protector peut détecter et configurer automatiquement les périphériques de magasin.

### Nettoyage de lecteurs encrassés

Data Protector peut utiliser des bandes nettoyantes pour nettoyer automatiquement les magasins et autres périphériques lorsqu'ils sont encrassés.

## Grandes bibliothèques

### Que sont les périphériques de bibliothèque ?

Les périphériques de bibliothèque sont des périphériques automatisés, également appelés chargeurs automatiques, échangeurs ou bibliothèques de bandes

magnéto-optiques. Dans Data Protector, la plupart des bibliothèques sont configurées comme bibliothèques SCSI. Elles contiennent un certain nombre de cartouches dans un référentiel de périphérique et peuvent posséder plusieurs lecteurs écrivant sur plusieurs supports à la fois.

Un périphérique de bibliothèque type dispose d'un ID SCSI pour chacun de ses lecteurs et un pour le mécanisme robotique de bibliothèque qui assure le transfert des supports entre les emplacements et les lecteurs. Par exemple, une bibliothèque équipée de quatre lecteurs possède cinq ID SCSI, quatre pour les lecteurs et un pour le mécanisme robotique.

Data Protector prend également en charge les bibliothèques silo, telles que HP StorageWorks, StorageTek/ACSL et ADIC/GRAU AML. La liste des périphériques pris en charge est accessible à l'adresse <http://www.hp.com/support/manuals>.

## Gestion des supports

L'interface utilisateur Data Protector fournit une vue de bibliothèque spéciale, qui simplifie la gestion des périphériques de bibliothèque.

Les supports d'un grand périphérique de bibliothèque peuvent tous appartenir au même pool de supports Data Protector ou être répartis sur plusieurs pools.

### Configuration d'une bibliothèque

Lorsque vous configurez un périphérique, vous définissez la plage d'emplacements que vous voulez attribuer à Data Protector. Cela permet de partager la bibliothèque avec d'autres applications. Les emplacements attribués peuvent contenir des supports vierges (neufs), des supports Data Protector ou d'autres types de support. Data Protector vérifie les supports dans les emplacements et affiche des informations les concernant dans la vue de la bibliothèque. Cela vous permet de visualiser tous les types de support, y compris ceux qui ne sont pas utilisés par Data Protector.

## Taille d'une bibliothèque

Les points suivants peuvent vous aider à estimer la taille de la bibliothèque dont vous avez besoin :

- Déterminez si les supports doivent être répartis sur plusieurs sites ou regroupés sur un même site.
- Calculez le nombre de supports requis. Reportez-vous à la section "[Mise en œuvre d'une stratégie de rotation des supports](#)" à la page 158.

## Partage d'une bibliothèque avec d'autres applications

Il est possible de partager un périphérique de bibliothèque avec d'autres applications stockant des données sur des supports de ce périphérique.

Vous pouvez sélectionner les lecteurs de la bibliothèque devant être utilisés dans Data Protector. Supposons que vous utilisiez une bibliothèque comprenant quatre lecteurs : vous pouvez dans ce cas décider d'utiliser deux de ces lecteurs dans Data Protector.

Vous pouvez sélectionner les emplacements de la bibliothèque devant être gérés dans Data Protector. Supposons que vous utilisiez une bibliothèque comprenant 60 emplacements : vous pouvez dans ce cas décider d'utiliser les emplacements 1 à 40 dans Data Protector. Les autres emplacements peuvent être utilisés et contrôlés par une autre application.

Le partage d'une bibliothèque entre plusieurs applications est fondamental dans le cas d'une grande bibliothèque HP et d'une bibliothèque silo (StorageTek/ACSL, ADIC/GRAU AML, etc.).

## Logements d'insertion/d'éjection

Les périphériques de bibliothèque disposent de logements d'insertion/éjection spéciaux que l'opérateur peut utiliser pour insérer des supports dans le périphérique et les en éjecter. Selon les périphériques, plusieurs logements d'insertion/d'éjection peuvent exister. Dans le cas d'un logement de bande unique, les supports sont insérés un par un, alors que dans le cas de logements de bande multiples, il est possible d'utiliser un nombre déterminé de logements dans une seule opération d'insertion/éjection.

Data Protector permet d'insérer/éjecter plusieurs supports en une seule étape. Par exemple, vous pouvez sélectionner 50 compartiments dans le périphérique et éjecter tous les supports en une seule opération. Data Protector éjecte automatiquement les supports dans le bon ordre pour que l'opérateur puisse retirer les supports du logement d'insertion/éjection.

Pour plus d'informations, reportez-vous à la documentation de votre périphérique.

## Prise en charge des codes-barres

Data Protector prend en charge les périphériques de bibliothèque équipés d'un lecteur de codes-barres. Dans ces périphériques, chaque support dispose d'un code-barres l'identifiant de manière unique.

## Avantages des codes-barres

Les fonctions d'identification des supports, d'étiquetage et de détection de bande nettoiyante donnent de meilleurs résultats lorsque Data Protector utilise les codes-barres.

- L'analyse des codes-barres des supports contenus dans un référentiel de périphérique permet d'accélérer la procédure : en effet, il n'est pas nécessaire que Data Protector charge les supports dans un lecteur et lise leur en-tête.
- Le code-barres est automatiquement lu par Data Protector et permet d'identifier le support.
- Une bande nettoiyante est automatiquement détectée si elle dispose d'un préfixe de code-barres CLN.
- Le code-barres fournit un ID unique à chaque support dans la base de données IDB. Vous ne pouvez pas avoir deux codes-barres identiques dans votre environnement.

---

### CONSEIL :

Le cas échéant, vous pouvez utiliser le code-barres comme étiquette du support pendant l'initialisation du support.

---

## Prise en charge des bandes nettoiyantes

HP Data Protector permet le nettoyage automatique des bandes sur la plupart des périphériques prenant en charge les bandes nettoiyantes. Une bande nettoiyante est utilisée automatiquement par Data Protector lorsqu'un événement "lecteur encrassé" provenant du périphérique est détecté.

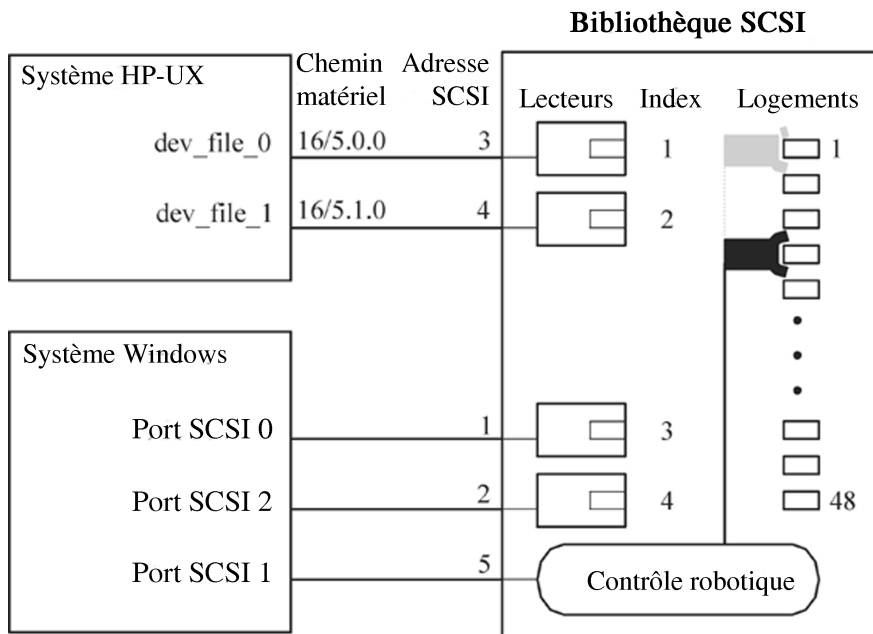
- Dans les bibliothèques SCSI, il est possible de définir quels emplacements contiendront une bande nettoiyante.
- Dans le cas de périphériques disposant d'un lecteur de codes-barres, Data Protector reconnaît automatiquement les codes-barres de la bande nettoiyante, à condition qu'ils contiennent le préfixe CLN.
- Pour les périphériques sans bande nettoiyante, une détection de lecteur encrassé entraîne une demande de nettoyage affichée dans la fenêtre du moniteur de session. L'opérateur doit ensuite nettoyer le périphérique manuellement.

Vous ne pouvez pas continuer votre sauvegarde si vous ne nettoyez pas le lecteur : la sauvegarde risque d'échouer car les données peuvent ne pas être correctement écrites ou stockées sur le support.

## Partage d'une bibliothèque entre plusieurs systèmes

### Qu'est-ce que le partage de bibliothèques ?

Le partage de périphériques vous permet de relier plusieurs lecteurs d'une bibliothèque physique à différents systèmes. Ces systèmes peuvent alors effectuer des sauvegardes locales dans la bibliothèque. Les performances de la sauvegarde en sont améliorées de manière significative et le trafic réseau réduit. Pour partager la bibliothèque, les lecteurs de la bibliothèque doivent pouvoir être reliés à des bus SCSI séparés. Dans le cas de bibliothèques hautes performances, le partage est particulièrement utile puisqu'il permet au lecteur de recevoir des données en mode continu à partir de plusieurs systèmes, améliorant ainsi les performances. Data Protector redirige en interne les commandes robotiques vers le système qui gère le robot.



**Figure 49 Connexion de lecteurs à plusieurs systèmes**

### Protocoles de contrôle et Agents de support Data Protector

Les lecteurs présents dans la bibliothèque doivent être capables de se connecter physiquement à différents systèmes équipés d'un Agent de support Data Protector (l'Agent général de support ou l'Agent de support NDMP).

Data Protector permet d'utiliser deux types de protocole pour le contrôle des lecteurs :

- SCSI — pour les lecteurs SCSI ou Fibre Channel.  
Le protocole est mis en œuvre à la fois dans l'Agent général de support et dans l'Agent de support NDMP.
- NDMP — pour les lecteurs dédiés NDMP.  
Ce protocole n'est mis en œuvre que dans l'Agent de support NDMP.

D'autre part, il existe quatre types de protocoles utilisés pour le contrôle du robot de bibliothèque :

- ADIC/GRAU — pour le robot de bibliothèque ADIC/GRAU
- StorageTek ACS — pour le robot de bibliothèque StorageTek ACS
- SCSI — pour le robot des autres bibliothèques
- NDMP — pour le robot NDMP

Les quatre protocoles de contrôle du robot de bibliothèque sont mis en œuvre à la fois dans l'Agent général de support et dans l'Agent de support NDMP.

## Contrôle des lecteurs

Tout système client Data Protector configuré pour contrôler un lecteur dans une bibliothèque (quels que soient le protocole de contrôle du lecteur et la plate-forme utilisés) peut communiquer avec n'importe quel système client Data Protector configuré pour contrôler le robot dans la bibliothèque (quels que soient le protocole de contrôle des robots et la plate-forme utilisés). Il est ainsi possible de partager les fichiers dans n'importe quelle bibliothèque gérée parmi les systèmes client Data Protector sur plusieurs plates-formes utilisant différents protocoles de robot et lecteur. 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 configurés pour les lecteurs dédiés NDMP). Dans tous les autres cas, les deux Agents de support Data Protector sont interchangeables.

Le [Tableau 10](#) à la page 185 présente l'Agent de support Data Protector (l'Agent général de support ou l'Agent de support NDMP) requis sur les systèmes client



configurés pour le contrôle des lecteurs d'une bibliothèque dotée de lecteurs partagés entre plusieurs systèmes client.

**Tableau 10 Agent de support Data Protector requis pour le contrôle des lecteurs**

	Protocole de contrôle du lecteur	
	NDMP	SCSI
<b>Protocole de contrôle du robot (ADIC/GRAU, StorageTek ACS, SCSI ou NDMP)</b>	Agent de support NDMP	Agent de support NDMP ou Agent général de support

### Contrôle du robot

Un système client Data Protector contrôlant le robot de bibliothèque peut être doté de l'Agent général de support ou l'Agent de support NDMP, quel que soit le type de protocole de lecteur (NDMP ou SCSI) utilisé avec les lecteurs dans la bibliothèque.

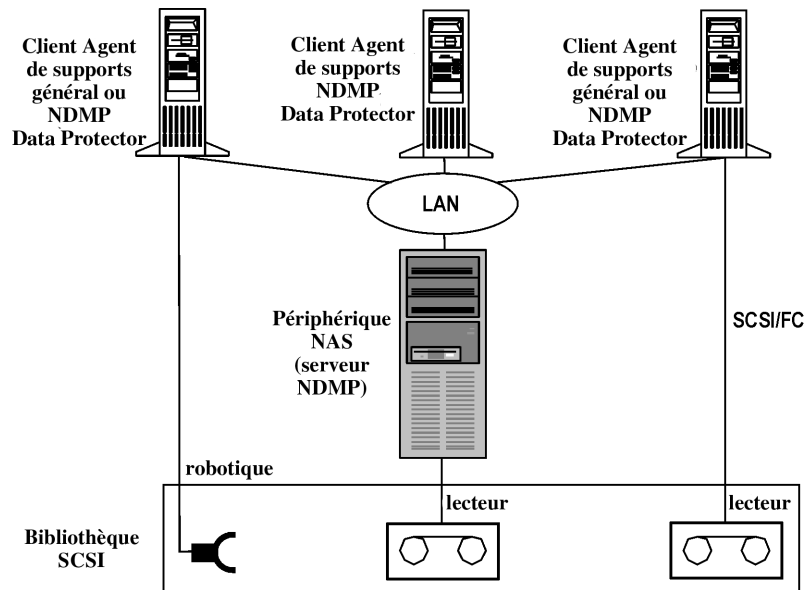
Le [Tableau 11](#) à la page 185 présente l'Agent de support Data Protector (l'Agent général de support ou l'Agent de support NDMP) requis sur un système client configuré pour le contrôle des robots d'une bibliothèque dotée de lecteurs partagés entre plusieurs systèmes client.

**Tableau 11 Agent de support Data Protector requis pour le contrôle des robots**

	Protocole de contrôle du robot			
	ADIC/GRAU	StorageTek ACS	SCSI	NDMP
<b>Protocole de contrôle du lecteur (NDMP ou SCSI)</b>	Agent de support NDMP ou Agent général de support	Agent de support NDMP ou Agent général de support	Agent de support NDMP ou Agent général de support	Agent de support NDMP ou Agent général de support

### Exemples de configurations

Les schémas entre la [Figure 50](#) à la page 186 et la [Figure 52](#) à la page 188 présentent des exemples de configurations de lecteurs partagés dans les bibliothèques et de distributions des Agents de support Data Protector dans les configurations en question.

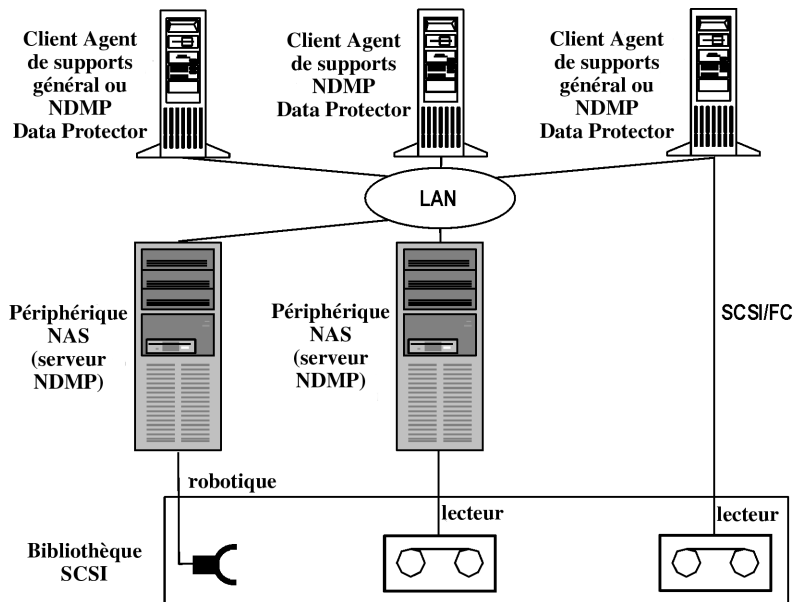


**Figure 50 Partage d'une bibliothèque SCSI (robot relié à un système client Data Protector)**

La Figure 50 à la page 186 présente une bibliothèque SCSI, ainsi que ses robots connectés au système client Data Protector et configurés sur ce dernier, sur lequel l'Agent général de support ou l'Agent de support NDMP est installé. Le protocole de contrôle du robot SCSI est utilisé par l'Agent général de support ou l'Agent de support NDMP sur le client. Le système client Data Protector auquel le robot est connecté peut également être relié à un ou plusieurs lecteurs.

Le lecteur dédié NDMP de la bibliothèque est configuré sur le système client Data Protector, sur lequel l'Agent de support NDMP est installé. L'Agent de support NDMP utilise le protocole de contrôle de lecteurs NDMP sur le client.

Un autre lecteur de la bibliothèque est relié au système client Data Protector et configuré sur ce dernier, sur lequel l'Agent général de support ou l'Agent de support NDMP est installé. Le protocole de contrôle du lecteur SCSI est utilisé par l'Agent général de support ou l'Agent de support NDMP sur le client.



**Figure 51 Partage d'une bibliothèque SCSI (robot relié à un serveur NDMP)**

La Figure 51 à la page 187 présente une bibliothèque SCSI, ainsi que ses robots connectés à un serveur NDMP et configurés sur le système client Data Protector, sur lequel l'Agent général de support ou l'Agent de support NDMP est installé. Le protocole de contrôle du robot SCSI est utilisé par l'Agent général de support ou l'Agent de support NDMP sur le client. Le serveur NDMP auquel le robot est connecté peut également être relié à un ou plusieurs lecteurs.

---

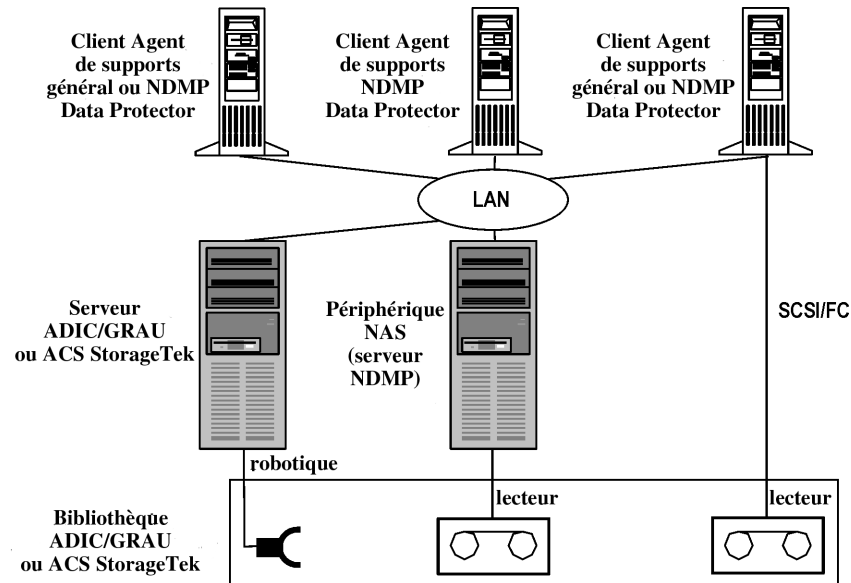
**! IMPORTANT :**

Si le serveur NDMP doté du robot est également relié à un lecteur dédié NDMP, le système client Data Protector sur lequel le robot et le lecteur dédié NDMP sont configurés, peut être pourvu uniquement de l'Agent de support NDMP, puisque le protocole de contrôle de lecteurs NDMP est utilisé pour le lecteur dédié NDMP.

Le lecteur dédié NDMP de la bibliothèque est configuré sur le système client Data Protector, sur lequel l'Agent de support NDMP est installé. L'Agent de support NDMP utilise le protocole de contrôle de lecteurs NDMP sur le client.

Un autre lecteur de la bibliothèque est relié au système client Data Protector et configuré sur ce dernier, sur lequel l'Agent général de support ou l'Agent de support

NDMP est installé. Le protocole de contrôle du lecteur SCSI est utilisé par l'Agent général de support ou l'Agent de support NDMP sur le client.



**Figure 52 Partage d'une bibliothèque ADIC/GRAU ou StorageTek ACS**

La Figure 52 à la page 188 présente une bibliothèque ADIC/GRAU ou StorageTek ACS, ainsi que ses robots connectés à un serveur ADIC/GRAU ou StorageTek ACS et configurés sur le système client Data Protector sur lequel l'Agent général de support ou l'Agent de support NDMP est installé. Le protocole de contrôle du robot ADIC/GRAU est utilisé par l'Agent général de support ou l'Agent de support NDMP sur le client. Le serveur ADIC/GRAU ou StorageTek ACS peut également être connecté à un ou plusieurs lecteurs.

Le lecteur dédié NDMP de la bibliothèque est configuré sur le système client Data Protector, sur lequel l'Agent de support NDMP est installé. L'Agent de support NDMP utilise le protocole de contrôle de lecteurs NDMP sur le client.

Un autre lecteur de la bibliothèque est relié au système client Data Protector et configuré sur ce dernier, sur lequel l'Agent général de support ou l'Agent de support NDMP est installé. Le protocole de contrôle du lecteur SCSI est utilisé par l'Agent général de support ou l'Agent de support NDMP sur le client.

## Data Protector et réseaux SAN

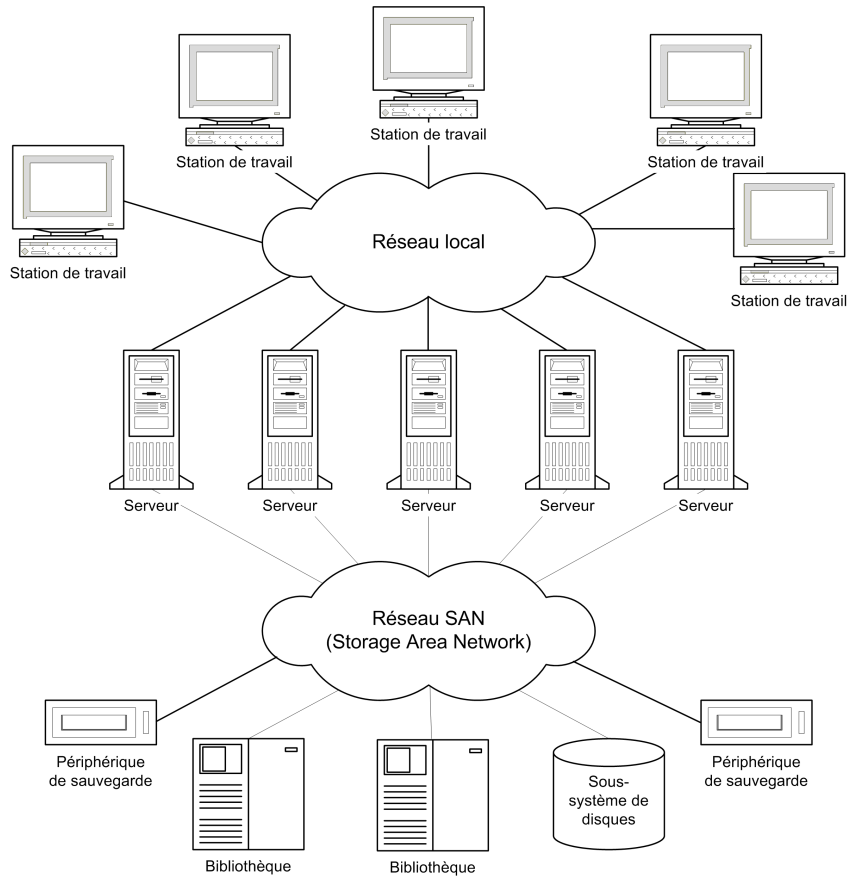
L'endroit où vous stockez les données de votre entreprise et la méthode de stockage que vous utilisez peuvent avoir un impact important sur vos activités. Pour la plupart des sociétés, l'information prend une importance croissante. Les utilisateurs doivent pouvoir accéder à des téraoctets de données à travers le réseau. La technologie Fibre Channel basée sur SAN mise en oeuvre par Data Protector vous offre la solution de stockage des données dont vous avez besoin.

### Storage Area Networks

Un Storage Area Network (SAN), illustré à la [Figure 53](#) à la page 190, représente une nouvelle approche de stockage en réseau, séparant la gestion de stockage de la gestion de serveur grâce à un réseau entièrement dédié au stockage.

Un SAN permet une *interconnectivité* de l'ensemble des ressources du réseau : les périphériques peuvent ainsi être partagés entre plusieurs systèmes client et le trafic de données ainsi que la disponibilité des périphériques sont améliorés.

Le concept SAN permet l'échange de données entre plusieurs serveurs et périphériques de stockage de données. Les serveurs peuvent accéder directement aux données de tout périphérique et n'ont pas besoin de transférer les données par le réseau local classique. Un SAN se compose de serveurs, de périphériques de sauvegarde, de baies de disques et d'autres nœuds, tous reliés par une connexion réseau rapide (généralement Fibre Channel). Ce réseau supplémentaire permet de décharger le réseau local classique, les opérations de stockage étant prises en charge par un réseau séparé.



**Figure 53 Storage Area Network**

## Fibre Channel

Fibre Channel est une norme ANSI pour l'interconnexion informatique à grande vitesse. Utilisant des câbles à fibre optique ou en cuivre, cette technologie permet la transmission bidirectionnelle de fichiers de données volumineux à une vitesse pouvant atteindre 4,25 gigabits par seconde, et peut être déployée entre des sites distants compris dans un périmètre de 30 km. La technologie Fibre Channel est à ce jour la solution la plus fiable et la plus performante pour le stockage, le transfert et la récupération des informations.

La technologie Fibre Channel relie les nœuds au moyen de trois topologies physiques différentes (présentant certaines variantes) :

- Point à point
- En boucle
- Commutée

Les topologies Fibre Channel point à point, en boucle et commutée peuvent être combinées pour répondre au mieux à vos exigences de connectivité et de croissance.

La liste des périphériques pris en charge est accessible à l'adresse <http://www.hp.com/support/manuals>.

## Topologie point à point

Cette topologie permet la connexion de deux nœuds, généralement un serveur et un périphérique de sauvegarde. Les principaux avantages sont l'amélioration des performances et l'augmentation des distances entre les nœuds.

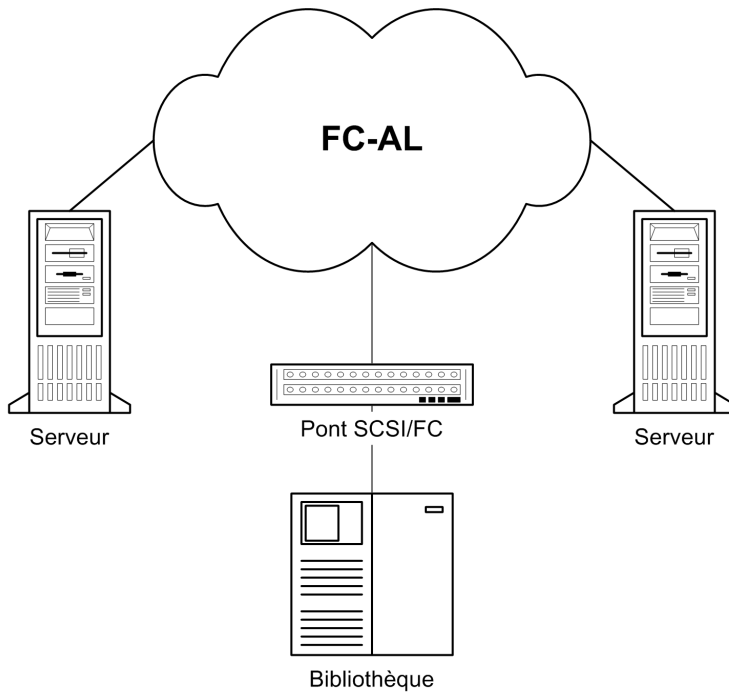
## Topologie en boucle

La topologie en boucle s'appuie sur la norme Fibre Channel Arbitrated Loop (FC-AL), qui permet de connecter jusqu'à 126 nœuds. Les nœuds comprennent les serveurs, les périphériques de sauvegarde, les concentrateurs et les commutateurs. Tout nœud d'une boucle peut communiquer avec un autre nœud de la boucle, et tous les nœuds partagent la même bande passante. Une boucle FC-AL est généralement mise en œuvre à l'aide d'un concentrateur FC-AL avec substitution automatique de port. La substitution automatique de port permet le branchement de nœuds à chaud à l'intérieur de la boucle.

## LIP

Une primitive LIP (Loop Initialization Primitive - protocole) peut être déclenchée pour plusieurs raisons, la plus courante étant l'apparition d'un nouveau périphérique. Le nouveau périphérique peut être un périphérique utilisé précédemment ayant été allumé ou un périphérique actif ayant été déplacé d'un port du commutateur à un autre. Une occurrence LIP peut provoquer une interruption inopportune d'une procédure en cours sur SAN, par exemple une opération de sauvegarde sur bande. Le bus SCSI reliant la passerelle SCSI/FC et le nœud (périphérique SCSI) est réinitialisé. Reportez-vous à la [Figure 54](#) à la page 192.

Lors d'une sauvegarde ou d'une restauration, la réinitialisation du bus SCSI est enregistrée comme erreur d'écriture. Data Protector abandonne toutes les opérations en cas d'erreur d'écriture. Dans le cas de sauvegardes, il est recommandé de copier les données déjà sauvegardées sur un support, puis de reformater le support et de redémarrer la sauvegarde.



**Figure 54 Protocole LIP (Loop Initialization Protocol)**

## Topologie commutée

La topologie commutée fournit une interconnectivité entre tous les nœuds reliés à un commutateur. Les commutateurs sont faciles à installer et à utiliser, le protocole Fibre Channel permettant l'autoconfiguration et l'autogestion. Les commutateurs détectent automatiquement les équipements connectés (nœuds, concentrateurs FC-AL ou tout autre commutateur FC) et s'autoconfigurent en conséquence. Les commutateurs fournissent aux nœuds connectés une bande passante proportionnée. La topologie commutée permet de brancher les nœuds à chaud.





#### REMARQUE :

Le branchement à chaud correspond à certaines capacités du protocole, telles que la réinitialisation, le rétablissement des communications, etc. N'oubliez pas que les transferts de données en cours sont interrompus pendant le branchement à chaud et que certains périphériques, tels que les périphériques à bande, ne gèrent pas cette fonctionnalité. Le fait de connecter ou de déconnecter les nœuds d'une boucle risque d'interrompre la procédure de sauvegarde ou de restauration et de faire échouer l'opération. Pour connecter ou déconnecter les nœuds d'une boucle, vérifiez qu'aucune sauvegarde ou restauration n'utilise le matériel associé.

## Partage de périphériques dans un SAN

Data Protector prend en charge le concept SAN dans la mesure où il permet à plusieurs systèmes de partager des périphériques de sauvegarde dans l'environnement SAN. Le même périphérique physique est accessible à partir de plusieurs systèmes. Tout système peut donc effectuer une sauvegarde locale sur ce périphérique ou tout autre périphérique. Les données étant transférées via le SAN, les sauvegardes n'ont pas besoin de bande passante sur votre réseau local classique. Ce type de sauvegarde est parfois désigné sous le nom de sauvegarde indépendante du réseau local. Les performances de la sauvegarde sont améliorées, la technologie Fibre Channel basée sur SAN offrant un débit supérieur à celui des technologies de réseau local.

Vous devez empêcher les systèmes dotés de plusieurs ordinateurs d'écrire sur le même périphérique en même temps. La situation est encore plus complexe lorsque les périphériques sont utilisés par plusieurs applications. L'accès aux périphériques doit être synchronisé entre tous les systèmes impliqués. Cette opération est effectuée grâce à des mécanismes de verrouillage.

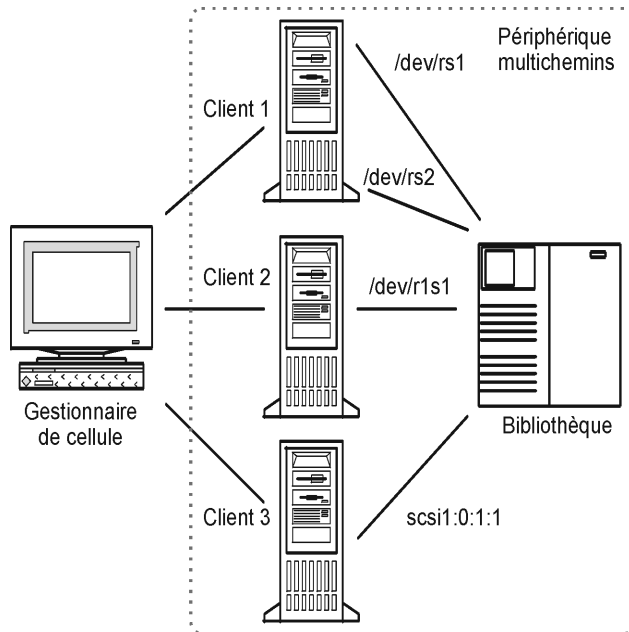
La technologie SAN représente un excellent moyen de gérer le robot d'une bibliothèque à partir de plusieurs systèmes. Elle vous offre la possibilité de gérer les robots à partir d'un même système (classique) ou d'autoriser chaque système utilisant la bibliothèque d'accéder directement aux robots, à condition que les requêtes robotiques soient synchronisées entre tous les systèmes impliqués.

## Configuration de plusieurs chemins vers des périphériques physiques

Un périphérique dans un environnement SAN est généralement connecté à différents clients et il est ainsi possible d'y accéder via plusieurs chemins, à savoir des noms de client et des adresses SCSI (fichiers de périphérique sur UNIX). Data Protector

peut utiliser l'un de ces chemins. Vous pouvez configurer tous les chemins d'accès à un périphérique physique sous la forme d'un périphérique logique unique (**périphérique MultiPath**).

Par exemple, un périphérique est connecté à `client1` et configuré en tant que `/dev/rs1` et `/dev/rs2`, sur `client2` en tant que `/dev/r1s1` et sur `client3` en tant que `scsi1:0:1:1`. Vous pouvez alors y accéder par quatre chemins : `client1:/dev/rs1`, `client1:/dev/rs2`, `client2:/dev/r1s1` et `client3:scsi1:0:1:1`. Un périphérique multichemins contient par conséquent les quatre chemins vers ce périphérique à bandes.



**Figure 55 Exemple de configuration multichemins**

### Utilité des chemins multiples

Les versions antérieures de Data Protector permettaient d'accéder à chaque périphérique à partir d'un seul client. Pour remédier à ce problème, plusieurs périphériques logiques devaient être configurés pour un périphérique physique utilisant un nom de verrouillage. Ainsi, si vous utilisiez des noms de verrouillage pour la configuration de l'accès à partir de différents systèmes vers un seul périphérique physique, vous deviez configurer tous les périphériques sur chaque système. Par exemple, pour 10 clients connectés à un seul périphérique, vous deviez configurer 10 périphériques avec le même nom de verrouillage. Cette version de Data Protector

permet de simplifier la configuration en configurant un seul périphérique multichemins pour l'ensemble des chemins.

Les périphériques multichemins augmentent la résilience des systèmes. Data Protector essaiera d'utiliser le premier chemin défini. Si tous les chemins sur un client sont inaccessibles, Data Protector essaiera d'utiliser les chemins sur le client suivant. La session est abandonnée si tous les chemins répertoriés sont indisponibles.

### Sélection des chemins

Pendant une session de sauvegarde, les chemins d'accès aux périphériques sont sélectionnés dans l'ordre défini à la configuration des périphériques, à moins qu'un hôte favori ne soit sélectionné dans la spécification de sauvegarde. Dans ce cas, le client favori est utilisé en premier.

Pendant une session de restauration, les chemins d'accès aux périphériques sont sélectionnés dans l'ordre suivant :

1. Chemins qui se trouvent sur le client sur lequel les objets sont restaurés, si *tous* les objets sont restaurés sur le même client cible
2. Chemins utilisés pour la sauvegarde
3. Autres chemins disponibles

Si l'accès direct à la bibliothèque est activé, les chemins locaux (chemins sur le client de destination) sont d'abord utilisés pour le contrôle des bibliothèques, quel que soit l'ordre de configuration.

### Compatibilité avec les versions antérieures

Les périphériques configurés avec les versions précédentes de Data Protector ne sont pas reconfigurés pendant une mise à niveau ; ils peuvent être utilisés comme dans les versions précédentes de Data Protector, sans aucune modification. Pour pouvoir utiliser la nouvelle fonctionnalité multichemins, vous devez reconfigurer les périphériques en périphériques multichemins.

### Verrouillage de périphérique

Le verrouillage de périphérique concerne les cas dans lesquels plusieurs applications utilisent le même périphérique et ceux dans lesquels Data Protector utilise un périphérique pour l'envoi de données et de commandes vers celui-ci à partir de plusieurs systèmes. Le but du verrouillage est de faire en sorte qu'un seul système à la fois communique avec un périphérique partagé entre plusieurs systèmes.

## Verrouillage de périphérique et applications multiples

Si Data Protector et au moins une autre application doivent utiliser le même périphérique à partir de plusieurs systèmes, le même mécanisme de verrouillage de périphérique (générique) doit être utilisé par chaque application. Ce mécanisme doit pouvoir fonctionner avec plusieurs applications. Ce mode n'est actuellement pas pris en charge par Data Protector. Si cela est nécessaire, des règles de fonctionnement doivent être appliquées pour garantir l'accès exclusif d'une application à tous les périphériques.

## Verrouillage de périphérique dans Data Protector

Si Data Protector est la seule application utilisant un lecteur, mais que ce lecteur doit être employé par plusieurs systèmes, vous devez utiliser le mécanisme de verrouillage de périphérique.

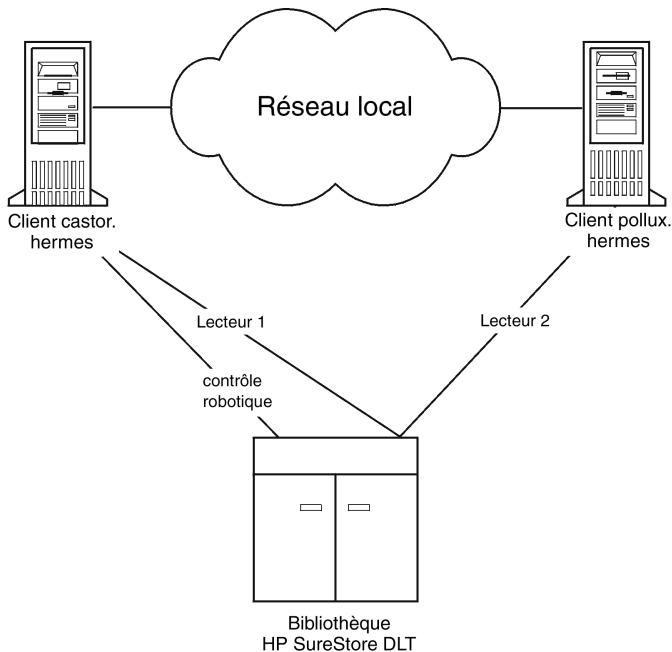
Si Data Protector est la seule application utilisant le contrôle robotique à partir de plusieurs systèmes, Data Protector gère la procédure en interne à condition que le contrôle de bibliothèque se trouve dans la même cellule que tous les systèmes devant la contrôler. Dans ce cas, la synchronisation de l'accès au périphérique est intégralement gérée en interne par Data Protector.

## Accès direct et indirect à la bibliothèque

Lors de la configuration de Data Protector associé à un périphérique de bibliothèque SCSI, les systèmes client peuvent accéder au robot de la bibliothèque de deux façons : accès direct et indirect à la bibliothèque.

## Accès indirect à la bibliothèque

Cette configuration peut être utilisée à la fois dans les réseaux SAN et dans les environnements de connexion directe type SCSI. Plusieurs systèmes peuvent accéder au robot de la bibliothèque en envoyant leur demande à un système client disposant d'un accès direct au robot de bibliothèque. C'est ce qu'on appelle l'accès indirect à la bibliothèque. Dans l'exemple illustré à la [Figure 56](#) à la page 197, deux systèmes client sont reliés à une bibliothèque multilecteurs DLT HP StorageWorks. Le système client `castor` contrôle le robot et le premier lecteur, tandis que le système client `pollux` contrôle le deuxième lecteur. Un Agent de support Data Protector sur `pollux` communique avec un processus en cours d'exécution sur `castor` pour faire fonctionner le robot. Cette fonctionnalité de partage de bibliothèque Data Protector est utilisée automatiquement lorsque les noms d'hôte de la bibliothèque et du lecteur sont différents.



**Figure 56 Accès indirect à la bibliothèque**

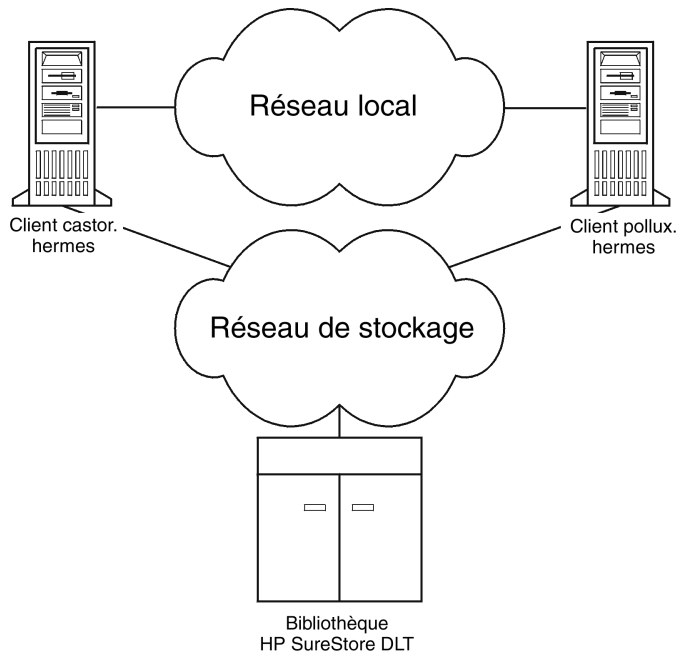
Notez que vous ne pouvez pas utiliser de bibliothèque partagée si le système client qui contrôle le robot, *castor* dans notre exemple, échoue.

## Accès direct à la bibliothèque

Lorsque le concept SAN est utilisé, Data Protector associé à une bibliothèque SCSI peut être configuré pour que chaque système client dispose de son propre accès aux lecteurs et au robot de la bibliothèque. On parle alors d'accès direct à la bibliothèque.

Il n'existe pas de "système client de contrôle" unique pour le robot : l'échec du système contrôlant le robot n'empêche pas les autres systèmes d'utiliser la bibliothèque. Cela est possible sans reconfiguration. Plusieurs systèmes client peuvent être utilisés pour contrôler le robot.

La [Figure 57](#) à la page 198 montre une bibliothèque multilecteurs DLT HP StorageWorks reliée à deux systèmes client via un SAN. Les deux systèmes client ont accès à la bibliothèque et aux lecteurs. Le protocole SCSI est utilisé pour les communications avec la bibliothèque.



**Figure 57 Accès direct à la bibliothèque**

## Partage de périphériques dans les clusters

La gestion de clusters, souvent utilisée en combinaison avec le concept SAN, est basée sur le partage de ressources réseau entre les nœuds (par exemple des noms réseau, des disques et des périphériques à bandes).

Les applications compatibles cluster peuvent être lancées à tout moment sur n'importe quel nœud dans un cluster (elles fonctionnent sur des hôtes virtuels). Pour effectuer une sauvegarde locale d'une telle application, vous devez configurer les périphériques disposant de noms d'hôtes virtuels à la place de noms de nœud réels. Configurez autant de périphériques physiques que vous le souhaitez, en utilisant le mécanisme de verrouillage de périphérique "Nom de verrouillage". Pour plus de détails, reportez-vous à la section "[Verrouillage de périphérique](#)" à la page 195.

## Lecteurs statiques

Les lecteurs statiques sont des périphériques configurés sur un nœud réel dans un cluster. Ils peuvent être utilisés pour sauvegarder des données à partir de systèmes possédant des disques non partagés. Ils ne sont cependant pas utiles pour les

sauvegardes d'applications compatibles cluster, puisque de telles applications peuvent être lancées à partir de n'importe quel nœud du cluster.

## Lecteurs flottants

Les lecteurs flottants sont des périphériques configurés sur un hôte virtuel, qui utilisent des noms de systèmes virtuels. Les lecteurs flottants doivent être configurés pour la sauvegarde d'applications compatibles cluster. Cela permet de s'assurer que, quel que soit le nœud du cluster sur lequel l'application s'exécute, Data Protector démarre toujours un Agent de support sur ce même nœud.





---

# 4 Utilisateurs et groupes d'utilisateurs

## Dans ce chapitre

Ce chapitre traite du système de sécurité, des utilisateurs, des groupes d'utilisateurs et des droits utilisateur dans Data Protector.

Il s'organise comme suit :

“Sécurité renforcée pour les utilisateurs Data Protector” à la page 201

“Utilisateurs et groupes d'utilisateurs” à la page 202

## Sécurité renforcée pour les utilisateurs Data Protector

Data Protector offre une fonction de sécurité avancée qui permet d'éviter qu'une sauvegarde ou une restauration de données non autorisée soit effectuée. Data Protector gère une sécurité consistant à interdire l'accès à certaines données aux utilisateurs non autorisés, à coder des données et à définir des groupes d'utilisateurs en fonction de leurs responsabilités.

Cette section décrit les différents points de sécurité liés à l'utilisation de Data Protector pour la sauvegarde de données, la restauration de données et le contrôle de l'avancement d'une session de sauvegarde.

## Accès à des données sauvegardées

Sauvegarder et restaurer des données revient à copier des données. Il est donc important de limiter l'accès à ces données aux utilisateurs autorisés.

Le système de sécurité Data Protector relatif aux utilisateurs est le suivant :

- Toute personne souhaitant utiliser Data Protector doit être définie comme utilisateur Data Protector.

## Visibilité des données sauvegardées

- Seul le propriétaire de la sauvegarde peut visualiser les données qu'il a sauvegardées. Les autres utilisateurs n'ont même pas la possibilité de déterminer si ces données ont été sauvegardées. Par exemple, lorsque l'opérateur de sauvegarde configure une sauvegarde, l'administrateur système et lui sont les seuls autorisés à visualiser et restaurer les données sauvegardées. Vous pouvez rendre des données visibles à d'autres utilisateurs en utilisant l'option **Public** de Data Protector. Pour plus d'informations, consultez l'aide en ligne de Data Protector.

## Utilisateurs et groupes d'utilisateurs

Pour pouvoir utiliser Data Protector, vous devez être ajouté à sa configuration en tant qu'utilisateur Data Protector disposant de certains privilèges. Notez que l'ajout d'un utilisateur ne constitue pas un prérequis pour la sauvegarde du système qu'il utilise.

Les utilisateurs sont réunis au sein de groupes d'utilisateurs ayant des droits spécifiques : par exemple, le droit de contrôler des sessions dans la cellule, de configurer des sauvegardes et de restaurer des fichiers.

### Groupes d'utilisateurs prédéfinis

Pour simplifier la configuration des sauvegardes, Data Protector fournit des groupes d'utilisateurs prédéfinis disposant de certains droits d'accès aux fonctionnalités du logiciel. Par exemple, seuls les membres du groupe d'utilisateurs admin peuvent accéder à l'ensemble des fonctionnalités de Data Protector. Par défaut, les opérateurs peuvent lancer et contrôler des sauvegardes.

---

#### CONSEIL :

Dans les petits environnements, une seule personne suffit pour exécuter toutes les tâches de sauvegarde. Elle doit appartenir au groupe d'utilisateurs admin de Data Protector. Dans ce cas, il n'est pas nécessaire d'ajouter d'autres utilisateurs à la configuration Data Protector.

---

En fonction de votre environnement, vous pouvez utiliser les groupes d'utilisateurs Data Protector par défaut, les modifier ou en créer d'autres.

## Administrateurs par défaut

Lors de l'installation, les utilisateurs suivants sont automatiquement ajoutés au groupe d'administrateurs Data Protector :

- l'utilisateur "root" UNIX du système Gestionnaire de cellule pour UNIX
- l'utilisateur qui installe Data Protector sur le système Gestionnaire de cellule Windows

Cela permet à ces derniers de configurer et d'utiliser l'intégralité des fonctionnalités de Data Protector. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "groupe d'utilisateurs, admin".

## Utilisation des groupes d'utilisateurs prédéfinis

Les groupes d'utilisateurs suivants sont définis par défaut dans Data Protector :

**Tableau 12 Groupes d'utilisateurs prédéfinis Data Protector**

Groupe d'utilisateurs	Droits d'accès
Admin	Autorisé à configurer Data Protector et à effectuer des sauvegardes, des restaurations et toute autre opération possible.
Opérateur	Autorisé à lancer des sauvegardes et à répondre aux demandes de montage.
Utilisateur final	Autorisé à restaurer ses propres objets. De plus, les utilisateurs peuvent contrôler les demandes de montage et y répondre lors de leurs propres sessions de restauration.



### REMARQUE :

Les fonctions d'administrateur confèrent un pouvoir important. Les membres du groupe d'utilisateurs admin Data Protector disposent de privilèges administrateur système sur tous les clients de la cellule Data Protector.

## Droits utilisateur Data Protector

Les utilisateurs de Data Protector disposent des droits utilisateur accordés au groupe auquel ils appartiennent. Par exemple, tous les membres du groupe d'utilisateurs admin disposent des droits du groupe d'utilisateurs admin Data Protector.

Lorsqu'un utilisateur est configuré depuis le domaine Windows, alors que Data Protector s'exécute sur le Gestionnaire de cellule UNIX, la configuration de cet utilisateur doit comporter le nom de domaine ou le groupe de caractères génériques " \* ".

Pour obtenir une description détaillée des droits utilisateur Data Protector propres à chaque groupe, consultez l'aide en ligne.

Par ailleurs, vous pouvez compléter la couche de sécurité utilisateur fournie par les groupes d'utilisateurs Data Protector avec des restrictions sur les opérations que peuvent effectuer les utilisateurs sur certains systèmes de la cellule. Pour configurer ces restrictions, utilisez le fichier `user_restrictions` situé sur le Gestionnaire de cellule. Elles s'appliquent uniquement aux membres des groupes d'utilisateurs Data Protector autres que Administrateur et Opérateur. Pour plus d'informations, reportez-vous à l'aide en ligne.

---

# 5 Base de données interne de Data Protector

## Dans ce chapitre

Ce chapitre décrit l'architecture de la base de données interne (IDB) de Data Protector, son utilisation et son fonctionnement. Vous y trouverez notamment des explications sur les différentes parties de la base de données et leurs enregistrements, des conseils sur la gestion de la croissance et des performances, ainsi que des formules pour calculer la taille de la base. Ces informations sont nécessaires pour pouvoir gérer la configuration et la maintenance de la base de données de manière efficace.

Il s'organise comme suit :

“A propos de la base de données IDB” à la page 205

“Architecture de la base de données IDB” à la page 207

“Fonctionnement de la base de données IDB” à la page 215

“Présentation de la gestion de la base de données IDB” à la page 218

“Croissance et performances de la base de données IDB” à la page 219

## A propos de la base de données IDB

### Qu'est-ce que la base de données interne (IDB) de Data Protector ?

La base de données IDB est une base intégrée, qui réside sur le Gestionnaire de cellule et permet d'identifier les données sauvegardées, les supports sur lesquels elles se trouvent, les résultats des sessions de sauvegarde, de restauration, de copie, de consolidation et de vérification d'objets et de gestion des supports ainsi que les périphériques et bibliothèques configurés.

## Pourquoi utiliser la base de données IDB ?

Les informations stockées dans l'IDB permettent d'effectuer les opérations suivantes :

- **Restauration rapide et facile** : Les informations stockées dans la base de données IDB vous permettent de retrouver rapidement les supports requis pour une restauration et d'accélérer ainsi considérablement le processus. Cette base de données vous permet également de parcourir aisément les fichiers et les répertoires à restaurer.
- **Gestion de la sauvegarde** : Les informations stockées dans la base de données IDB vous permettent de vérifier comment se sont déroulées les sauvegardes. Vous pouvez également configurer plusieurs rapports au moyen de la fonction de reporting de Data Protector.
- **Gestion des supports** : Les informations stockées dans la base de données IDB permettent d'allouer des supports pendant les sessions de sauvegarde, de copie et de consolidation d'objets, d'effectuer un suivi des attributs de supports et des emplacements des supports dans les bibliothèques de bandes, et de regrouper des supports dans des pools différents.
- **Gestion du cryptage/décryptage** : Les informations stockées dans la base de données IDB permettent à Data Protector d'allouer des clés de cryptage aux sessions de sauvegarde ou de copie d'objets, et de fournir la clé de décryptage requise pour la restauration des objets de sauvegardes cryptées.

## A propos de la taille et de la croissance de l'IDB

La base de données IDB peut grossir énormément et avoir un impact important sur les performances des sauvegardes et sur le système du Gestionnaire de cellule. Par conséquent, l'administrateur Data Protector doit comprendre l'IDB et, en fonction des besoins, décider de la nature et de la durée de validité des informations qu'elle contient. Il est le rôle de l'administrateur d'établir un équilibre entre le temps de restauration et la fonctionnalité d'une part, et la taille et la croissance de la base de données IDB d'autre part. Data Protector propose deux paramètres principaux pour vous aider à équilibrer vos besoins : **niveau de journalisation** et **protection de catalogue**. Reportez-vous également à la section "[Croissance et performances de la base de données IDB](#)" à la page 219.

## Base de données IDB dans le Gestionnaire de cellule Windows

### Emplacement IDB

La base de données interne sur le Gestionnaire de cellule Windows se trouve dans le répertoire `données_programme_Data_Protector\db40` (Windows Server 2008) ou `répertoire_Data_Protector\db40` (autres systèmes Windows).

## Format IDB

La base de données IDB dans le Gestionnaire de cellule Windows stocke toutes les informations textuelles au format Unicode codé sur deux octets. Cette base de données IDB grossit donc un peu plus rapidement que celle du Gestionnaire de cellule UNIX qui stocke les informations au format ASCII.

Le format Unicode permet de prendre totalement en charge les noms de fichier et les messages localisés dans d'autres langues.

## Base de données IDB dans le Gestionnaire de cellule UNIX

### emplacement IDB

Dans un Gestionnaire de cellule UNIX, la base de données IDB est située dans le répertoire `/var/opt/omni/server/db40`.

### format IDB

La base de données IDB dans le Gestionnaire de cellule HP-UX ou Solaris stocke toutes les informations textuelles au format ASCII codé sur un ou plusieurs octets.

Le format ASCII limite la prise en charge des noms de fichier et des messages localisés dans d'autres langues. Lorsque vous sauvegardez des fichiers avec des noms dans un format codé sur deux octets (Unicode, par exemple), ces noms sont convertis au format ASCII et peuvent ne pas s'afficher correctement dans l'interface utilisateur de Data Protector. Toutefois, les fichiers et les noms de fichier sont restaurés correctement.

Pour plus de détails, reportez-vous à la section "[Internationalisation](#)" à la page 365.

## Base de données IDB dans un environnement Manager-of-Managers

Dans un environnement Manager-of-Managers, la base de données de gestion centralisée des supports (CMMDB) permet de partager des supports et périphériques entre plusieurs cellules. Pour plus d'informations sur les fonctionnalités du gestionnaire MoM, reportez-vous à la section "[Environnements d'entreprise](#)" à la page 44.

## Architecture de la base de données IDB

La base de données IDB est constituée des éléments suivants :

- La MMDB (base de données de gestion des supports)

- La CDB (base de données catalogue), elle-même divisée en deux parties : les noms de fichier et les autres enregistrements CDB
- Les DCBF (fichiers binaires de catalogue des détails)
- Les SMBF (fichiers binaires de messages de session)
- Les SIBF (fichiers binaires des intégrations sans serveur pour l'intégration NDMP)
- Les banques de clés de cryptage

Chaque élément de la base de données IDB stocke des informations spécifiques de Data Protector (enregistrements), agit différemment sur la taille et la croissance de la base de données IDB et se trouve dans un répertoire distinct du Gestionnaire de cellule. Reportez-vous à la [Figure 58](#) à la page 209.

Pour obtenir des informations et des conseils sur l'optimisation de la robustesse par le déplacement de certains répertoires de la base de données IDB, recherchez l'entrée suivante dans l'index de l'aide en ligne : "fiabilité de l'IDB".

### Technologie sous-jacente

Les éléments MMDB et CDB sont mis en œuvre à l'aide d'une base de données intégrée composée d'espaces de table. Celle-ci est contrôlée par le processus du serveur de base de données RDS. Tous les changements apportés à la MMDB et à la CDB sont mis à jour à l'aide de journaux de transactions. Ces derniers sont stockés dans le répertoire `db40\logfiles\syslog`. Les éléments CDB (objets et positions) et MMDB représentent le cœur de la base de données IDB.

Les éléments DCBF, SMBF et SIBF de la base de données IDB sont des fichiers binaires. Les mises à jour se font directement (pas de transaction).



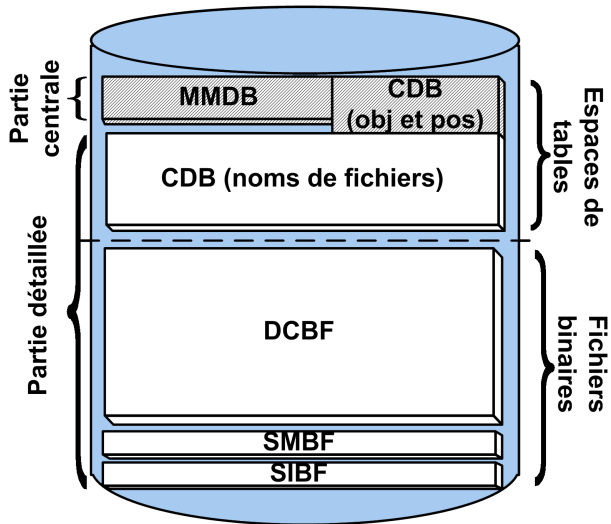


Figure 58 Parties de l'IDB

## Base de données de gestion des supports (MMDB)

### Enregistrements MMDB

La base de données de gestion des supports stocke des informations concernant les éléments suivants :

- les périphériques, les bibliothèques, les lecteurs de bibliothèque et les logements faisant partie de la configuration
- les supports Data Protector
- les pools et magasins de supports faisant partie de la configuration

### MMDB, taille et croissance

La taille de la base de données de gestion des supports n'augmente pas énormément. La plus grande partie de la base de données est généralement occupée par des informations concernant les supports Data Protector. L'espace utilisé est d'environ 30 Mo. Pour plus de détails, reportez-vous à la section "[Estimation de la taille de l'IDB](#)" à la page 226.

### Emplacement de la MMDB

La MMDB se trouve dans le répertoire suivant :

- Sous Windows Server 2008 : `données_programme_Data_Protector\db40\datafiles\mmdb`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\db40\datafiles\mmdb`
- Sur les systèmes UNIX : `/var/opt/omni/server/db40/datafiles/mmdb`

## Base de données catalogue (CDB)

### Enregistrements CDB

La base de données catalogue stocke des informations concernant :

- Les sessions de sauvegarde, de restauration, de copie, de consolidation, de vérification d'objets et de gestion des supports. Il s'agit d'une copie des informations envoyées à la fenêtre du moniteur Data Protector.
- Les objets sauvegardés, leurs versions et les copies d'objet. Dans le cas des versions d'objets cryptés, les identificateurs de clés (IDClé-IDBanque) sont également stockés.
- Les emplacements des objets sauvegardés sur les supports. Pour chaque objet sauvegardé, Data Protector stocke des informations concernant les supports et les segments de données utilisés pour la sauvegarde. Il en va de même pour les copies d'objet et les mises en miroir d'objet.
- Les chemins d'accès des fichiers sauvegardés (noms de fichier) ainsi que les noms des systèmes client. Les noms de fichier ne sont stockés qu'une fois par système client. Les noms de fichier créés entre les sauvegardes sont ajoutés à la base de données catalogue.

### Taille et croissance des noms de fichier

Les noms de fichier représentent la partie la plus importante de la base de données catalogue et celle qui s'accroît le plus vite. Ils occupent en général 20 % de l'ensemble de la base de données. La croissance de la partie consacrée aux noms de fichier est proportionnelle à la croissance et aux variations de l'environnement de sauvegarde, et non au nombre de sauvegardes.

Sur un Gestionnaire de cellule HP-UX ou Solaris, un fichier ou répertoire occupe entre 50 et 70 octets dans la base de données IDB, tandis que sur un Gestionnaire de cellule Windows, il occupe entre 70 et 100 octets.

Les noms de fichier sont stockés dans le fichier `fnames.dat` et dans certains autres fichiers, selon leur longueur. La taille maximum de chacun de ces fichiers est de 2 Go. Vous êtes informé dès que l'un de ces fichiers commence à être saturé ; cela

vous permet d'ajouter de nouveaux fichiers afin d'étendre la taille de la partie noms de fichier de la base de données IDB.

### Taille et croissance de la CDB (objets et positions)

Les enregistrements de la base de données catalogue autres que les noms de fichier occupent très peu d'espace dans la base de données IDB. Un environnement de sauvegarde de taille moyenne occupe généralement environ 100 Mo. Pour plus d'informations, reportez-vous à la section "[Estimation de la taille de l'IDB](#)" à la page 226.

### Emplacement de la CDB

La CDB se trouve dans le répertoire suivant :

- Sous Windows Server 2008 : `données_programme_Data_Protector\db40\datafiles\cdb`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\db40\datafiles\cdb`
- Sur les systèmes UNIX : `/var/opt/omni/server/db40/datafiles/cdb`

## Fichiers binaires de catalogue des détails (DCBF)

### Informations sur les DCBF

La partie des fichiers binaires de catalogue des détails stocke les informations concernant les versions de fichier. Ces informations se rapportent aux fichiers sauvegardés. Il s'agit notamment de la taille des fichiers, de l'heure de modification, de la protection, des attributs, etc.

Un fichier binaire DC (catalogue des détails) est créé pour chaque support Data Protector utilisé pour une sauvegarde. Lorsque les informations du support sont écrasées, l'ancien fichier binaire est remplacé par un nouveau.

### DCBF, taille et croissance

Dans un environnement où l'option **Journaliser tout** est fréquemment utilisée pour la sauvegarde des systèmes de fichiers, les DCBF occupent la plus grande partie de la base de données IDB (en général 80 %). La taille des DCBF peut se calculer avec la formule suivante : *fichier\_dcbf\_en\_octets* égale approximativement *nbre\_de\_fichiers\_sur\_bande x 30\_octets*. Il est possible d'utiliser le niveau de journalisation et la protection de catalogue pour spécifier ce qui est réellement stocké dans la base de données IDB et pour combien de temps. Reportez-vous à la

section “[Croissance et performances de la base de données IDB : paramètres clés réglables](#)” à la page 220.

Par défaut, un répertoire DC, `db40\dcbf`, est configuré pour les fichiers binaires DC. Sa taille maximale par défaut est de 16 Go. Vous pouvez créer d'autres répertoires DC, les copier sur différents disques du Gestionnaire de cellule et augmenter ainsi la taille de la base de données IDB. Le nombre maximum de répertoires pris en charge par cellule est de 50.

## Emplacement des DCBF

Par défaut, les DCBF se trouvent dans le répertoire suivant :

- Sous Windows Server 2008 : `données_programme_Data_Protector\db40\dcbf`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\db40\dcbf`
- Sur les systèmes UNIX : `/var/opt/omni/server/db40/dcbf`

Assurez-vous qu'il y a suffisamment d'espace dans le Gestionnaire de cellule. Si ce n'est pas le cas, déplacez le répertoire DC. Vous pouvez créer d'autres répertoires DC et les placer sur différents disques. Ne créez plusieurs répertoires DC que si le nombre de fichiers binaires de DC par support devient très important (plusieurs milliers) ou si vous avez des problèmes d'espace. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : “répertoires DC”.

## Fichiers binaires de messages de session (SMBF)

### Enregistrements SMBF

La partie des fichiers binaires de messages de session stocke les messages de session générés pendant les sessions Data Protector. Chaque session génère un fichier binaire. Les fichiers sont regroupés par année et par mois.

### SMBF, taille et croissance

La taille des SMBF dépend des éléments suivants :

- Nombre de sessions exécutées, puisqu'un fichier binaire est créé pour chaque session.
- Nombre de messages dans une session. Un message de session occupe environ 200 octets sur un système Windows et 130 octets sur un système UNIX. Vous pouvez modifier le nombre de messages affichés au moment des opérations de sauvegarde, de restauration et de gestion des supports au moyen de l'option

Niveau de rapport. Ce paramètre influe également sur le nombre de messages stockés dans la base de données IDB. Pour plus d'informations, reportez-vous à l'aide en ligne.

## Emplacement des SMBF

Les SMBF se trouvent dans le répertoire suivant :

- Sous Windows Server 2008 : `données_programme_Data_Protector\db40\msg`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\db40\msg`
- Sur les systèmes UNIX : `/var/opt/omni/server/db40/msg`

Vous pouvez déplacer le répertoire en modifiant l'option globale `SessionMessageDir`. Pour plus d'informations sur le fichier d'options globales Data Protector, reportez-vous au *Guide de dépannage HP Data Protector* *Guide de dépannage HP Data Protector*.

## Fichiers binaires d'intégrations sans serveur (SIBF)

### Enregistrements SIBF

Les fichiers SIBF stockent les données de restauration NDMP brutes. Ces données sont nécessaires à la restauration d'objets NDMP.

### SIBF, taille et croissance

Les SIBF n'augmentent pas énormément. Pour plus d'informations, reportez-vous à la section "[Estimation de la taille de l'IDB](#)" à la page 226. Dans le cas des sauvegardes NDMP, les fichiers SMBF grossissent proportionnellement au nombre d'objets sauvegardés. Environ 3 Ko sont utilisés par objet sauvegardé.

### Emplacement des SIBF

Les SIBF se trouvent dans le répertoire suivant :

- Sous Windows Server 2008 : `données_programme_Data_Protector\db40\meta`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\db40\meta`
- Sur les systèmes UNIX : `/var/opt/omni/server/db40/meta`

## Banque de clés de cryptage et fichiers catalogue

Toutes les clés créées, manuellement ou automatiquement, pendant les sauvegardes cryptées sont stockées dans une banque de clés. Les clés peuvent également être utilisées pour les sessions de copie et de vérification d'objets et de restauration. Dans le cas d'un cryptage matériel, elles peuvent en outre être utilisées pour les sessions de consolidation d'objets.

En cas de cryptage sur logiciel, les identificateurs de clés (chacun constitué d'un IDClé et d'un IDBanque) sont mappés vers les versions d'objets cryptés. Ce mappage est stocké dans la base de données catalogue. Différents objets sur un support peuvent avoir des clés de cryptage (logiciel) différentes.

Pour le cryptage matériel, les identificateurs de clés sont mappés vers l'ID de support de données et ces mappages sont stockés dans un fichier catalogue. Ce fichier contient les informations nécessaires pour pouvoir exporter un support crypté vers une autre cellule.

### Emplacement de la banque de clés

La banque de clés se trouve dans le répertoire suivant :

- Sous Windows Server 2008 : `données_programme_Data_Protector\db40\keystore`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\db40\keystore`
- Sur les systèmes UNIX : `/var/opt/omni/server/db40/keystore`

### Emplacement du fichier catalogue

Les fichiers catalogue se trouvent dans le répertoire suivant :

- Sous Windows Server 2008 : `données_programme_Data_Protector\db40\keystore\catalog`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\db40\keystore\catalog`
- Sur les systèmes UNIX : `/var/opt/omni/server/db40/keystore/catalog`

# Fonctionnement de la base de données IDB

## Pendant la sauvegarde

Lorsqu'une session de sauvegarde démarre, un enregistrement de session est créé dans la base de données IDB. Un enregistrement de version d'objet est également créé pour chaque objet et chaque objet miroir de la session. Tous ces enregistrements sont stockés dans la CDB et dotés de plusieurs attributs. Si le cryptage logiciel a été demandé pour la sauvegarde, les clés de cryptage actives des entités concernées (hôtes) sont extraites de la banque de clés et utilisées pour la sauvegarde, et les identificateurs de clés (IDClé-IDBanque) sont reliées aux versions d'objets et incluses dans les enregistrements de la CDB. Les mappages des hôtes aux IDClé-IDBanque sont également stockés dans un catalogue de la banque de clés.

Le Gestionnaire de session de sauvegarde met à jour les supports au cours d'une sauvegarde. Tous les enregistrements de support sont stockés dans la MMDB et sont alloués à une sauvegarde en fonction des stratégies définies. Si les supports concernés se trouvent dans des lecteurs pour lesquels le cryptage matériel a été demandé, les clés de cryptage actives des entités (supports) sont d'abord extraites de la banque de clés. Les mappages des supports aux IDClé-IDBanque sont enregistrés dans un catalogue de la banque de clés et écrits sur les supports.

Lorsqu'un segment de données est écrit sur la bande, puis sur un segment de catalogue, un enregistrement d'emplacement de support est stocké dans la CDB pour chaque version d'objet faisant partie de ce segment de données. De plus, le catalogue est stocké dans le fichier binaire de catalogue des détails. Pour chaque support Data Protector, un fichier binaire de catalogue des détails est mis à jour. Le nom du fichier binaire de catalogue des détails est `IDsupport_horodatage.dat`. Si les données d'un support sont écrasées pendant une sauvegarde, son ancien fichier binaire de catalogue des détails est remplacé par un nouveau.

Tous les messages de session générés pendant les sauvegardes sont stockés dans des fichiers binaires de messages de session (partie SMBF).

Si la journalisation des transactions est activée, la sauvegarde de la base de données IDB supprime les anciens journaux de transactions et crée de nouveaux journaux nécessaires à la récupération de la base de données IDB.

## Pendant la restauration

Lors de la configuration de la restauration, Data Protector réalise une série de requêtes dans les parties CDB et DCBF afin de permettre aux utilisateurs d'explorer les systèmes

de fichiers virtuels des données sauvegardées. Ces requêtes d'exploration se divisent en deux étapes. La première consiste à sélectionner un objet spécifique (système de fichiers ou lecteur logique). Si cet objet contient plusieurs versions et/ou copies de sauvegarde stockées, cette opération peut prendre un certain temps car Data Protector analyse les DCBF afin de créer un cache de recherche qui lui permettra d'explorer les répertoires par la suite. La deuxième étape consiste à explorer les répertoires.

Une fois les versions de fichiers spécifiques sélectionnées, Data Protector détermine les supports nécessaires et localise les enregistrements d'emplacement de support utilisés par les fichiers sélectionnés. Ces supports sont ensuite lus par les Agents de support et les données sont envoyées aux Agents de disque qui restaurent les fichiers sélectionnés. Si les supports concernés ont subi un cryptage matériel, l'Agent de support recherche d'abord les identificateurs de clés (IDClé-IDBanque) et demande la clé qui est extraite de la banque de clés par le serveur gestionnaire de clés (KMS - Key Management Server).

Si les sauvegardes concernées ont subi un cryptage logiciel, lorsque les Agents de disque reçoivent les données cryptées, ils soumettent les IDClé-IDBanque détectés au KMS et demandent les clés de décryptage appropriées, qui sont extraites de la banque de clés.

## Pendant la copie ou la consolidation d'objets

Pendant une session de copie ou de consolidation d'objet, les processus qui s'exécutent sont les mêmes que pendant une session de sauvegarde et de restauration. Les données sont lues à partir du support source comme si elles étaient restaurées, puis écrites sur le support cible comme si elles étaient sauvegardées. Une session de copie ou de consolidation d'objet a la même incidence sur le fonctionnement de l'IDB que les opérations de sauvegarde et de restauration. Pour plus d'informations, reportez-vous aux sections "[Pendant la sauvegarde](#)" à la page 215 et "[Pendant la restauration](#)" à la page 215. Cela ne s'applique pas à la consolidation d'objet avec cryptage logiciel, dans la mesure où elle n'est pas prise en charge.

## Pendant la vérification d'objet

Pendant une session de vérification d'objets, les mêmes processus s'exécutent au cours d'une session de restauration. Les données sont lues à partir du support source comme si elles étaient restaurées, puis envoyées aux Agents de disque de l'hôte sur lequel la vérification est effectuée. Une session de vérification d'objet a la même incidence sur le fonctionnement de l'IDB qu'une opération de restauration. Tous les messages de session générés durant les sessions de vérification sont stockés dans des fichiers binaires de messages de session. Pour plus d'informations, reportez-vous à la section "[Pendant la restauration](#)" à la page 215.



## Exportation de supports

Lorsqu'un support est exporté, s'il contient des données cryptées, les clés appropriées dans la banque de clés sont exportées dans un fichier .csv sur le Gestionnaire de cellule. Ce fichier est requis pour que l'importation du support dans une autre cellule soit correctement réalisée.

Par ailleurs, plusieurs éléments sont supprimés.

### Emplacement du répertoire d'exportation de clés

L'emplacement du répertoire d'exportation de clés de cryptage est le suivant :

- Sous Windows Server 2008 : `données_programme_Data_Protector\Config\Server\export\keys`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\Config\Server\export\keys`
- Sur les systèmes UNIX : `/var/opt/omni/server/export/keys`

### Éléments supprimés

Les éléments suivants sont supprimés :

- Tous les enregistrements d'emplacement de support pour ce support sont supprimés de la partie CDB.
- Tous les objets et toutes les copies d'objet qui ne figurent plus sur un autre support sont supprimés de la partie CDB.
- Les sessions obsolètes (dont les supports ont été soit écrasés soit exportés) de plus de 30 jours sont supprimées (cela peut être modifié au moyen de la variable `KeepSession` du fichier d'options globales). Les messages de ces sessions sont également supprimés.
- L'enregistrement du support est supprimé de la partie MMDB et le fichier binaire de catalogue des détails correspondant est supprimé des DCBF.

## Suppression du catalogue des détails

Lorsque le catalogue des détails est supprimé pour un support donné, le fichier binaire DC correspondant l'est également. Le même résultat est obtenu en supprimant la protection de catalogue pour toutes les versions et toutes les copies d'objet sur ce support (le fichier binaire sera supprimé au cours de la prochaine maintenance quotidienne des fichiers binaires de catalogue des détails). Tous les autres

enregistrements restent dans la CDB et dans la MMDB et il est possible de lancer la restauration depuis l'un de ces supports (l'exploration, en revanche, est impossible).

## Purge des noms de fichier

Les fichiers binaires de catalogue des détails indiquent si un fichier donné est sauvegardé sur un support associé ou non, mais les noms de fichier sont stockés dans la CDB. Un nom de fichier est considéré comme "utilisé" s'il est indiqué comme sauvegardé dans au moins un fichier binaire de catalogue des détails. Avec le temps, il se peut qu'un grand nombre de noms de fichiers soient inutilisés. Pour les supprimer, Data Protector analyse l'ensemble des fichiers binaires de catalogue des détails, puis supprime les noms de fichier non utilisés.

## Purge des versions de fichier

Lorsque la protection de catalogue de toutes les versions d'objet stockées sur un support spécifique expire, la maintenance quotidienne automatique des fichiers binaires DC supprime le fichier binaire correspondant.

# Présentation de la gestion de la base de données IDB

## Configuration de la base de données IDB

L'une des étapes les plus importantes de la configuration de votre environnement de sauvegarde Data Protector est la configuration de la base de données IDB. La configuration initiale vous permet de définir les stratégies internes concernant la taille de la base de données IDB, l'emplacement de ses répertoires, la sauvegarde de la base nécessaire si celle-ci est endommagée ou après un sinistre, ainsi que la configuration de ses rapports et notifications.

---

### ❗ IMPORTANT :

Il est fortement recommandé de planifier une sauvegarde quotidienne de la base de données IDB. La définition d'une spécification de sauvegarde pour la base de données IDB fait également partie de la configuration de cette dernière.

---

## Maintenance de la base de données IDB

Une fois la base de données IDB configurée, sa maintenance est réduite à son minimum, en agissant principalement sur les notifications et les rapports.

## Récupération de la base de données IDB

Une récupération de la base de données IDB est nécessaire si certains de ses fichiers sont manquants ou endommagés. La procédure de récupération dépend du niveau d'altération.

Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "base de données IDB, récupération".

# Croissance et performances de la base de données IDB

Pour configurer et entretenir correctement la base de données IDB, il est indispensable de bien comprendre les facteurs clés qui influent sur la croissance et les performances de la base de données IDB, ainsi que les principaux paramètres réglables que vous pouvez adapter à vos besoins. Ainsi, vous serez en mesure d'appréhender le plus efficacement possible la croissance et les performances de la base de données IDB.

## Facteurs clés des performances et de la croissance de l'IDB

Les facteurs clés des performances et de la croissance de la base de données IDB sont les suivants :

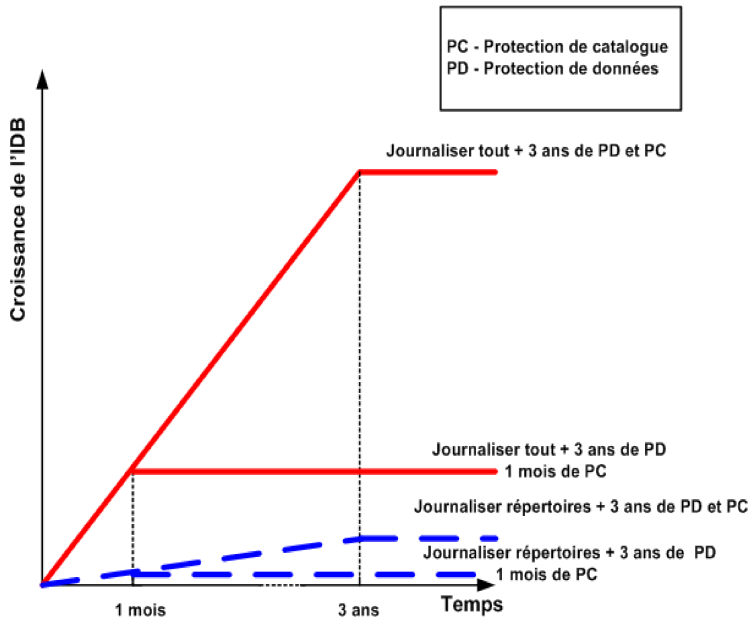
- Paramètres de niveau de journalisation. Le niveau de journalisation indique le volume de données écrites dans l'IDB pendant la sauvegarde. Plus le niveau de journalisation utilisé est détaillé, plus l'IDB est influencée. Pour plus de détails, reportez-vous à la section "[Croissance et performances de la base de données IDB : paramètres clés réglables](#)" à la page 220.
- Paramètre de protection de catalogue. La protection de catalogue détermine la durée pendant laquelle les informations sur les données sauvegardées sont disponibles dans l'IDB. Plus la période de protection de catalogue définie est longue, plus l'IDB est influencée. Pour plus de détails, reportez-vous à la section "[Croissance et performances de la base de données IDB : paramètres clés réglables](#)" à la page 220.
- Nombre de fichiers sauvegardés. Data Protector garde une trace de chaque fichier et de la version associée. L'incidence des différents types de sauvegarde sur la base de données IDB n'est pas la même. Pour obtenir des informations sur

les différents types de sauvegarde, reportez-vous à la section “[Sauvegardes complètes et incrémentales](#)” à la page 72.

- Nombre de sauvegardes  
Plus les sauvegardes sont fréquentes, plus le volume d'informations stockées dans la base de données IDB est important.
- Variations du système de fichiers Le nombre de fichiers créés et supprimés entre les sauvegardes peut avoir un effet considérable sur la croissance de la partie des noms de fichier de l'IDB. Le [rapport sur les variations du système](#) peut vous apporter des informations utiles. Pour éviter un accroissement de la base de données IDB dû aux variations du système de fichiers, utilisez le niveau de journalisation `Journaliser répertoires`.
- Croissance de votre environnement de sauvegarde. Le nombre de systèmes en cours de sauvegarde dans la cellule agit sur la croissance de la base de données IDB. Il est conseillé de planifier la croissance de votre environnement de sauvegarde.
- L'encodage de caractères utilisé pour vos noms de fichier (applicable sous UNIX uniquement). Selon le codage du nom de fichier, un caractère du nom de fichier peut occuper d'un à trois octets dans l'IDB. Par exemple, les noms de fichier codés via le système Shift-JIS occupent jusqu'à trois octets dans l'IDB, alors que les noms de fichier codés en ASCII pur n'occupent qu'un octet. Le codage des caractères est pertinent pour la croissance de la partie noms de fichier de l'IDB sous UNIX (sous Windows, tous les caractères occupent deux octets dans l'IDB).
- Nombre de copies d'objet et de miroirs d'objet. Plus vous créez de copies et de miroirs d'objets, plus la quantité d'informations stockée dans l'IDB augmente. Dans le cas des copies et des miroirs d'objets, l'IDB stocke les mêmes informations que pour les objets sauvegardés, à l'exception des noms de fichiers.

## Croissance et performances de la base de données IDB : paramètres clés réglables

Le niveau de journalisation et la protection de catalogue sont les principaux facteurs de croissance et de performances de la base de données IDB. Leur impact sur la base de données IDB dépend des paramètres utilisés. Pour obtenir une représentation graphique de l'effet des différents paramètres en termes de niveau de journalisation et de protection de catalogue, reportez-vous à la [Figure 59](#) à la page 221.



**Figure 59 Influence du niveau de journalisation et de la protection de catalogue sur la croissance de la base de données IDB**

## Niveau de journalisation comme paramètre clé réglable de l'IDB

### Qu'est-ce que le niveau de journalisation ?

Le niveau de journalisation détermine la quantité de détails figurant dans l'IDB pour les fichiers et répertoires sauvegardés. Vous pouvez toujours restaurer vos données, sans tenir compte du niveau de journalisation utilisé pendant la sauvegarde.

Data Protector propose quatre niveaux de journalisation permettant de contrôler la quantité de détails sur les fichiers et répertoires enregistrés dans l'IDB :

- Journaliser tout**      Journalise toutes les informations détaillées sur les fichiers et répertoires sauvegardés (noms, versions et attributs).
- Fichiers journaux**      Journalise toutes les informations détaillées sur les fichiers et répertoires sauvegardés (noms et versions). Cela représente environ 30 % des informations détaillées sur les fichiers et répertoires sauvegardés.

<b>Journaliser répertoires</b>	Journalise toutes les informations détaillées sur les répertoires sauvegardés (noms, versions et attributs). Cela représente environ 10 % de toutes les informations détaillées sur les fichiers et répertoires sauvegardés.
<b>Pas de journalisation</b>	Aucune information sur les fichiers et répertoires sauvegardés n'est enregistrée dans la base de données IDB.

Les différents paramètres agissent sur la croissance de la base de données IDB, la vitesse de sauvegarde et la capacité d'exploration des données.

## Impact sur les performances

Le niveau de journalisation indique le volume des données enregistrées dans la base de données IDB pendant une sauvegarde. Il agit également sur la vitesse de la base de données IDB et donc sur le processus de sauvegarde.

## Niveau de journalisation et exploration pour la restauration

Lorsque vous changez le niveau des informations stockées, vous modifiez vos possibilités d'exploration des fichiers à l'aide de l'interface Data Protector pendant une restauration. Si l'option `Pas de journalisation` est sélectionnée, l'exploration est impossible ; si l'option `Journaliser répertoires` est sélectionnée, l'exploration des répertoires est possible ; si l'option `Journaliser fichiers` est sélectionnée, vous pouvez explorer les fichiers et les répertoires, mais les attributs de fichier (taille, dates de création et de modification, etc.) ne sont pas affichées.

Il vous est toujours possible de restaurer vos données, quelque soit le niveau de journalisation données :

- Au lieu d'explorer vos données, vous pouvez toujours sélectionner manuellement un fichier à restaurer (si vous connaissez le nom du fichier).
- Vous pouvez également récupérer des informations sur les données sauvegardées à partir des supports.

## Niveau de journalisation et vitesse de restauration

La vitesse de restauration est approximativement la même lorsque les options `Journaliser tout`, `Journaliser répertoires` ou `Journaliser fichiers` sont sélectionnées.

Si l'option `Pas de journalisation` est sélectionnée, la vitesse de restauration peut être plus lente en cas de restauration de fichiers individuels. C'est dû au fait

que Data Protector doit lire toutes les données depuis le début d'un objet avant de trouver un fichier à restaurer.

Dans le cas d'une restauration complète du système, l'objet doit de toute façon être intégralement lu. Les paramètres de niveau de journalisation ne jouent donc pas un rôle très important.

## Protection de catalogue comme paramètre clé réglable de l'IDB

### Qu'est-ce que la protection de catalogue ?

La protection de catalogue détermine la durée pendant laquelle les informations sur les données sauvegardées sont disponibles dans l'IDB. Cette notion diffère de la protection des données, qui détermine la durée pendant laquelle les données sauvegardées sont disponibles sur le support lui-même. Si aucune protection de catalogue n'est définie, la restauration des données reste possible. Toutefois vous ne pourrez pas les explorer via l'interface Data Protector.

La protection de catalogue est basée sur le principe que les dernières données stockées sont les plus importantes et les plus utilisées. Les anciens fichiers sont rarement recherchés, il est donc moins gênant que leur recherche prenne plus de temps.

### Protection du catalogue expirée

Lorsque la protection de catalogue arrive à expiration, les informations ne sont pas immédiatement supprimées de l'IDB. Data Protector les supprime automatiquement une fois par jour. Les informations de l'IDB étant organisées par support, la protection de catalogue doit arriver à expiration pour tous les objets du support afin que les données soient entièrement supprimées.

### Impact sur les performances

Les paramètres de protection de catalogue n'ont aucun effet sur les performances de la sauvegarde.

### Protection de catalogue et restauration

Lorsque la protection de catalogue arrive à expiration, les données sont restaurées comme si elles avaient été sauvegardées avec l'option `Pas de journalisation`. Reportez-vous à la section "[Niveau de journalisation comme paramètre clé réglable de l'IDB](#)" à la page 221.

## Utilisation recommandée du niveau de journalisation et de la protection de catalogue

### Utiliser toujours la protection de catalogue

Définissez toujours un niveau raisonnable de protection de catalogue, . excepté lorsque l'option `Pas de journalisation` est sélectionnée (dans ce cas, la protection de catalogue ne s'applique pas).

Si vous définissez la protection de catalogue sur `Permanent`, les informations de l'IDB ne sont supprimées que lorsque les supports sont exportés ou supprimés. Dans ce cas, la taille de l'IDB augmente de manière linéaire jusqu'à la fin de la période de protection des données, même si le nombre de fichiers de la cellule ne change pas. Par exemple, si la période de protection des données est d'un an et que les supports sont recyclés, la croissance significative de l'IDB s'arrête au bout d'un an. L'ajout de nouveaux catalogues équivaut approximativement à la suppression des anciens. Si la protection de catalogue est définie sur quatre semaines, la croissance significative de l'IDB s'arrête au bout de quatre semaines. Dans ce cas, l'IDB est 13 fois plus volumineuse si la protection de catalogue définie est d'un an.

Il est recommandé de définir la protection de catalogue de sorte qu'elle couvre au moins la dernière sauvegarde complète. Vous pouvez par exemple la définir sur 8 semaines pour les sauvegardes complètes et sur une semaine pour les sauvegardes incrémentales.

### Utiliser différents niveaux de journalisation dans la même cellule

Une cellule est souvent constituée de serveurs de messagerie (ou équivalents) qui génèrent quotidiennement un grand nombre de fichiers, de serveurs de bases de données qui stockent toutes les informations dans un groupe de fichiers et de stations de travail utilisateur. Les variations de ces systèmes étant assez différentes, il est très difficile de conseiller un réglage qui leur conviendrait à tous. Il est donc recommandé de créer plusieurs spécifications de sauvegarde avec les paramètres de niveau de journalisation suivants :

- Pour les serveurs de messagerie, choisissez l'option `Journaliser répertoires`.
- Pour les serveurs de base de données, aucune journalisation n'est nécessaire puisqu'ils possèdent leurs propres règles de restauration. Par conséquent, utilisez l'option `Pas de journalisation`.
- Pour les stations de travail ou les serveurs de fichiers, les options `Journaliser tout` ou `Journaliser fichiers` permettent la recherche et la restauration de différentes versions de fichiers. Lorsque l'option `Journaliser répertoires`



ou `Pas de journalisation` est sélectionnée pour une sauvegarde, vous pouvez importer les catalogues à partir des supports, ce qui vous offre la possibilité d'explorer l'objet sélectionné en relativement peu de temps. Pour plus d'informations sur l'importation de catalogues à partir des supports, recherchez l'entrée suivante dans l'index de l'aide en ligne : "importation, catalogues à partir de supports".

### Niveaux de journalisation différents pour les copies d'objet

Les objets sauvegardés et les copies ou les miroirs de ces objets peuvent présenter le même niveau de journalisation ou un niveau de journalisation différent. Selon votre stratégie de sauvegarde, le niveau de journalisation sélectionné pour les copies d'objet peut être plus ou moins détaillé que celui des objets sources.

Par exemple, vous pouvez spécifier l'option `Pas de journalisation` pour les miroirs d'objet si vous créez ces miroirs simplement pour garantir l'aboutissement d'une session de sauvegarde. Vous pouvez aussi choisir l'option `Pas de journalisation` pour un objet sauvegarde afin d'augmenter les performances de l'opération de sauvegarde, puis choisir l'option `Journaliser tout` pour cet objet au cours d'une session de copie d'objet ultérieure.

### Particularités des petites cellules

Si le nombre de fichiers d'une cellule est peu important et n'évolue pas (un million de fichiers ou moins) et si les systèmes de la cellule réalisent les activités professionnelles habituelles, vous pouvez toujours utiliser l'option par défaut de Data Protector, `Journaliser tout`. Cependant, vous devez être attentif à la croissance de l'IDB et définir un niveau raisonnable de protection de catalogue.

### Particularités des grandes cellules

Si le nombre de fichiers atteint plusieurs dizaines de millions ou que des dizaines de milliers de fichiers sont générés par jour alors que vous avez sélectionné l'option `Journaliser tout`, la vitesse de sauvegarde et la croissance de l'IDB vont rapidement devenir problématiques. Dans une telle situation, vous avez la possibilité de :

- Réduire le niveau de journalisation au niveau le plus bas possible. Le fait de sélectionner l'option `Journaliser fichiers` peut diviser la taille de l'IDB par trois et l'option `Journaliser répertoires` environ par dix. Cela dépend bien sûr de la nature des systèmes de fichiers de la cellule.
- Réduire la protection de catalogue au minimum.
- Diviser la cellule en deux. Enfin, vous pouvez également créer une autre base de données IDB et y rediriger la moitié des systèmes.

Vous pouvez configurer le rapport sur les variations du système afin d'obtenir des informations sur les variations de la croissance des noms de fichier sur un client particulier.

## Estimation de la taille de l'IDB

Si vous effectuez principalement des sauvegardes de systèmes de fichiers, la base de données IDB peut, dans certaines conditions, atteindre une taille significative (supérieure à 16 Go). Si vous réalisez des sauvegardes d'images disque ou de bases de données en ligne, l'IDB ne devrait pas dépasser 2 Go.

Pour estimer la taille de l'IDB, utilisez l'outil de planification de capacité de la base de données interne, qui se trouve dans le composant `Documentation en anglais` (`guides`, `aide`). Lors de l'installation, cet outil est stocké dans l'emplacement suivant :

- **Systemes UNIX :**

```
/opt/omni/doc/C/IDB_capacity_planning.xls
```

- **Systemes Windows :**

```
répertoire_Data_Protector\docs\IDB_capacity_planning.xls
```

Cet outil permet également d'estimer la taille de l'IDB dans les environnements comportant des bases de données en ligne (Oracle, SAP R/3).

---

# 6 Gestion des services

## Dans ce chapitre

Grâce à la gestion des services, à la génération de rapports et au contrôle, les administrateurs sont en mesure de gérer plus efficacement leurs environnements de sauvegarde. Ce chapitre décrit les concepts de base de la gestion des services et présente ses avantages tant pour la configuration autonome de Data Protector que pour son intégration aux produits de gestion de services de HP.

Il s'organise comme suit :

“Généralités” à la page 227

“Fonctionnalité Data Protector native” à la page 228

## Généralités

Les services informatiques des entreprises font de plus en plus appel aux outils, techniques et méthodes de gestion des services pour fixer leurs objectifs en termes de niveau de service, évaluer leurs prestations par rapport à ces objectifs et justifier leur expansion future.

Les groupes informatiques devant gérer le risque de perte de données, la sauvegarde et la récupération de données sont des éléments essentiels dans la prestation et la gestion des services informatiques. Erreur des utilisateurs, virus, accès non autorisé aux données, défaillance occasionnelle du périphérique de stockage : autant d'éléments qui menacent en permanence les données. Or, une perte de données stratégiques peut coûter à l'entreprise des sommes considérables pour chaque heure d'indisponibilité.

Les utilisateurs, en revanche, considèrent parfois la sauvegarde des données comme une opération qui, pendant son exécution, peut ralentir ou empêcher leur accès à certains services. Néanmoins, sans cette activité essentielle, la disponibilité permanente et en temps voulu des services peut être réellement compromise.

Si toutes les données sont menacées, toutes n'ont pas les mêmes exigences en termes de capacité de récupération. Ainsi, les départements informatiques doivent assurer pour les données stratégiques un niveau de protection supérieur à celui des données moins essentielles, et ce à un coût réduit.

Les évaluations et les rapports de gestion des services comptent parmi les principaux outils que les responsables des services informatiques peuvent utiliser pour démontrer la valeur fournie à l'entreprise ainsi que pour conserver des structures de coûts compétitives. Les fournisseurs de services utilisent des accords sur le niveau de service (SLA) afin de définir les objectifs de disponibilité et de performances et de fixer ainsi les attentes des parties.

Un contrôle permanent et la génération périodique de rapports sont nécessaires pour savoir si les dispositions du SLA sont respectées. Data Protector offre en standard des outils de surveillance, de notification et de génération de rapports permettant de documenter les opérations de sauvegarde et de récupération. L'intégration à d'autres produits de gestion des services permet de regrouper les vues, les données de performance et les autres fonctionnalités dans une seule et même console, ce qui vous donne un meilleur aperçu de la prestation globale de services informatiques.

Data Protector fournit aux responsables des services informatiques des données essentielles pour le contrôle et la planification fonctionnels des opérations de sauvegarde et de récupération des données. Ces données peuvent être utilisées dans les activités consistant à planifier la disponibilité du service et la récupération, lesquelles sont fondamentales en cas de signature d'accords de service. De plus, les informations fournies par Data Protector peuvent servir à mettre en place des modèles de gestion des coûts et de facturation interne afin de permettre une véritable gestion financière du service informatique.

## Data Protector et la gestion des services

Data Protector offre des fonctions de gestion des services et peut être associé à des applications de gestion des services, telles que HP Operations Manager pour Windows.

Dans Data Protector, on distingue deux catégories de gestion des services : native et résultant de l'intégration d'autres applications. Les éléments de chaque catégorie sont détaillés plus loin dans ce chapitre.

## Fonctionnalité Data Protector native

La fonctionnalité décrite dans les sections suivantes est fournie en standard avec Data Protector.

## Fonctions principales

- Data Protector a été conçu pour assurer le suivi du temps écoulé pour les opérations clés et pour enregistrer ces données ainsi que leur volume à l'aide de l'API Application Response Measurement version 2.0 (API ARM 2.0). L'enregistrement de ces données peut être effectué à l'aide de HP Performance Agent (PA).
- Le contrôle intégré des sessions en cours permet de réagir instantanément aux événements survenant dans votre environnement de sauvegarde.
- Le moteur de notification et de génération de rapports intégré de Data Protector permet de recevoir des rapports concis ainsi que des avertissements immédiats sous différents formats (ASCII, HTML et formats compatibles tableurs) et selon différentes méthodes : e-mail, SNMP, diffusion (disponible uniquement sous Windows), enregistrement dans un fichier et envoi vers une commande externe. Le moteur de notification intégré de Data Protector étant en mesure d'envoyer des avertissements via SNMP, il est possible d'intégrer quasiment toutes les applications capables de recevoir des interruptions SNMP.
- Le système d'audit de session de sauvegarde de Data Protector stocke des informations concernant toutes les tâches de sauvegarde effectuées sur de longues périodes pour l'ensemble de la cellule Data Protector ; sur demande, il fournit ces informations complètes dans un format imprimable à des fins d'audit et d'administration.
- L'intégration de Data Protector à HP Operations Manager software permet de recevoir des avertissements de Data Protector sur la console OM et d'effectuer des actions automatiques.
- La capacité de Data Protector d'envoyer les événements majeurs et critiques au journal d'événements Windows ouvre la voie à toute une série de possibilités d'intégration très utiles.
- L'intégration avec HP Operations Manager pour Windows (OMW) permet un transfert automatique des événements majeurs et critiques de Data Protector vers la console OMW. Vous pouvez paramétrer des actions automatiques destinées à réagir aux pannes dans l'environnement de sauvegarde.
- Grâce à sa fonction intégrée de génération de rapports Java en ligne, Data Protector vous permet de créer des rapports en ligne depuis n'importe quel point du réseau (même à distance) sans que l'interface utilisateur Data Protector ne soit nécessairement installée sur votre ordinateur local. Vous devez disposer pour cela d'un navigateur Web.

## Application Response Measurement version 2.0 (API ARM 2.0)

### Qu'est-ce que l'API ARM ?

L'API ARM est une norme de plus en plus utilisée pour la mesure du temps de réponse de bout en bout des transactions dans les environnements distribués. Les applications qui utilisent l'API ARM se comportent comme des sources d'informations de temps de réponse (et aussi d'informations fournies par l'utilisateur pouvant être pertinentes pour une transaction particulière) pour les outils de contrôle et de gestion de systèmes compatibles ARM, tels que HP Performance Agent (PA).

**Tableau 13 Fonctionnalité ARM**

<b>Description de la transaction (ARM 1.0)</b>	<b>Données supplémentaires envoyées vers ARM (ARM 2.0)</b>	<b>Utilisation</b>
Durée de la session de spécification de sauvegarde	Données traitées [Mo]	Planification de la disponibilité et de la récupération. Facturation interne.
Durée de la session de sauvegarde d'un objet	Données traitées [Mo]	Planification de la disponibilité et de la récupération. Facturation interne.
Durée de la session de restauration	Données récupérées [Mo]	Planification de la disponibilité et de la récupération
Durée de la vérification de la base de données IDB	Taille de la base de données IDB [Mo]	Gestion de l'architecture Data Protector
Durée de la purge de la base de données IDB	Volume de la base de données IDB après la purge et nombre d'enregistrements purgés	Gestion de l'architecture Data Protector

Data Protector disposant déjà de l'ARM, il est relativement facile de l'associer à une application comme PA prenant en charge l'API ARM. Sur les plates-formes Windows, cela se fait de manière entièrement automatique. Lorsque Data Protector est installé sur un système où PA se trouve déjà (ou vice versa), les données de transaction

apparaissent immédiatement dans PA et HP Performance Manager (PM). Sous HP-UX, vous devez créer un lien d'un répertoire Data Protector vers un répertoire ARM (`libarm`). Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "intégration ARM, installation".

## Intégration avec le logiciel HP Operations Manager

### Fonctionnalités de l'intégration de HP avec OM

Data Protector s'intègre au logiciel HP Operations Manager (OM). OM simplifie la gestion des grands environnements en permettant à l'opérateur de contrôler et d'administrer le réseau et les applications à partir d'un seul point. Une fois que Data Protector est intégré à l'environnement OM, l'administrateur réseau peut immédiatement voir si une erreur survient lors de la sauvegarde et réagir en fonction des informations données. Les messages Data Protector peuvent s'afficher dans la fenêtre OM prévue à cet effet.

### Fonctionnalités du logiciel HP Operations Manager pour Windows

Le logiciel HP Operations Manager pour Windows (OMW) présente les caractéristiques suivantes :

- Data Protector enregistre dans le journal d'événements Windows tous les messages majeurs et critiques apparaissant lors d'une sauvegarde, d'une restauration ou de toute autre opération. Le logiciel HP Operations Manager pour Windows (OMW) utilise ensuite ces événements et les transfère vers la console OMW pour qu'un opérateur puisse agir en conséquence.
- Contrôle des services  
OMW contrôle tous les services Data Protector s'exécutant sur le Gestionnaire de cellule ainsi que tout système client Data Protector. En cas de dysfonctionnement de l'un des ces services, OMW en avertit immédiatement l'opérateur. OMW peut également être configuré de manière à ce qu'il tente automatiquement de relancer le service défectueux.

## Interruptions SNMP

Les interruptions SNMP permettent à une application de gestion des services de recevoir et de traiter un message d'interruption SNMP lorsqu'un événement Data Protector se produit ou lorsqu'une interruption SNMP est envoyée suite au déclenchement d'un mécanisme de vérification et de maintenance Data Protector. Pour plus d'informations sur le journal d'événements de Data Protector, recherchez

l'entrée suivante dans l'index de l'aide en ligne : “SNMP, méthodes d'envoi de rapports”.

## Moniteur

Élément de l'interface utilisateur de Data Protector, le moniteur Data Protector permet de superviser les sessions de sauvegarde, de restauration et de gestion des supports en cours et d'en corriger les erreurs. Via le moniteur, vous pouvez surveiller toutes les sessions d'une cellule et visualiser les messages détaillés ainsi que l'état actuel de ces sessions. Dans un environnement multicellules, vous pouvez afficher les sessions qui fonctionnent sur des systèmes informatiques installés dans d'autres cellules. Depuis l'interface utilisateur du moniteur, vous pouvez abandonner une session de sauvegarde, de restauration ou de gestion des supports ou encore répondre à des demandes de montage.

Si vous utilisez le Manager-of-Managers, vous pouvez contrôler les sessions de plusieurs cellules simultanément à partir d'une seule interface utilisateur.

## Génération de rapports et notification

La fonction de génération de rapports de Data Protector est un outil puissant, personnalisable et souple grâce auquel vous pouvez administrer et planifier votre environnement de sauvegarde. Data Protector a toujours intégré un large éventail de rapports exploités par les administrateurs pour gérer les systèmes Gestionnaire de cellule. Désormais, les fournisseurs de services informatiques peuvent utiliser ces mêmes rapports pour indiquer si les dispositions du SLA concernant la sécurité des données sont respectées. Parmi les rapports intégrés spécifiquement dédiés à la gestion du niveau de service, citons :

- Rapports d'inventaire/d'état, comme le rapport `host_not_conf`, qui contient des informations sur les systèmes non protégés, le rapport `dl_sched`, qui répertorie toutes les sauvegardes, les copies d'objet et les consolidations d'objet planifiées, et le rapport `media_list`, qui fait l'inventaire des supports.
- Rapports d'utilisation des capacités, comme le rapport sur la licence, qui décrit l'utilisation de la licence Data Protector, et le rapport `dev_unused`, qui répertorie les périphériques non utilisés pour une sauvegarde, une copie d'objet ou une consolidation d'objet (disponibles).
- Rapports de problèmes, comme le rapport `session_statistics`, qui contient des informations sur les échecs de sessions de sauvegarde, de copie ou de consolidation. L'administrateur peut recevoir une fois par heure, par jour ou par semaine un e-mail décrivant les tâches qui ont échoué et les raisons de leur échec.



Les fonctions de notification et de génération de rapports qui ont toujours fait partie intégrante du Gestionnaire de cellule (et qui ont été largement étendues depuis les versions antérieures) vous permettent également d'exécuter les opérations suivantes :

- Choisir parmi de nombreux rapports prédéfinis (notamment les rapports sur les sessions dans une période donnée, les rapports sur la base de données IDB et les rapports d'utilisation des périphériques).
- Spécifier vos propres paramètres pour ces rapports (comme les périodes, les spécifications de sauvegarde, de copie ou de consolidation et les groupes de sauvegardes).
- Faire un choix parmi les divers formats de sortie (tels que ASCII, HTML et formats compatibles tableurs).
- Planifier ces rapports avec le planificateur Data Protector intégré.
- Déclencher l'envoi des rapports en fonction d'événements donnés (dysfonctionnement d'un périphérique, demandes de montage ou fin de sessions, par exemple).
- Choisir parmi différents modes d'envoi la façon dont ces rapports doivent vous parvenir : e-mail, SNMP, diffusion (disponible uniquement sous Windows), enregistrement dans un fichier et envoi vers une commande externe.

Vous pouvez combiner la plupart de ces différents paramètres : formats, modes de réception, planifications et déclenchements.

En voici quelques exemples :

### Exemples de rapports et de notifications

- Tous les matins, à 7:00, un rapport est créé sur toutes les sessions de sauvegarde, de copie ou de consolidation effectuées au cours des dernières 24 heures, puis envoyé au format ASCII par e-mail à la boîte aux lettres de l'administrateur. De plus, ce même rapport est enregistré sur votre serveur Web dans un fichier au format HTML, de sorte que d'autres utilisateurs peuvent avoir accès à ces informations.
- Dans le cas d'une défaillance d'un périphérique ou d'une demande de montage, un message de diffusion est immédiatement envoyé à la station de travail Windows de l'administrateur et une commande externe est déclenchée pour avertir l'administrateur sur son récepteur de poche.
- A la fin d'une session de sauvegarde, chaque utilisateur final dont le système a été sauvegardé reçoit un e-mail au format ASCII, dans lequel figure le rapport d'état de sauvegarde.

## Journalisation et notification des événements

Le journal d'événements Data Protector est un référentiel central contenant l'ensemble des notifications ayant trait à Data Protector. Les événements consignés dans le journal d'événements Data Protector sont déclenchés par les processus ou par les utilisateurs. Le moteur de notification intégré de Data Protector envoie des avertissements ou active le mécanisme de génération de rapports de Data Protector en fonction des entrées du journal. Le journal d'événements constitue la principale source d'informations pour les rapports de conformité au SLA dans Data Protector ou dans les applications de gestion HP. Les entrées du journal contribuent non seulement à la génération de rapports, mais aussi à l'envoi d'informations aux applications de gestion HP via le SPI (SMART Plug-in) Data Protector, ce qui leur permet de déclencher des actions préventives ou correctives (pour plus de détails, voir l'exemple sous 3.1).

Le moteur de notification intégré de Data Protector étant en mesure d'envoyer des avertissements via SNMP, il est possible d'intégrer à Data Protector quasiment toutes les applications capables de recevoir des interruptions SNMP. L'intégration à HP Operations Manager est un exemple d'une mise en oeuvre fondée sur les interruptions SNMP.

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 d'événements** Data Protector au moyen de l'observateur de journal d'événements.

## Fichiers journaux Data Protector

Certaines applications de gestion des services, telles que le logiciel HP Operations Manager, vous permettent de spécifier les fichiers journaux à contrôler pour une entrée de journal spécifique et le moment où ce contrôle doit être effectué. Si l'entrée spécifiée est détectée dans le fichier, une action peut être définie. Dans OM, cette opération est appelée *Encapsulation du fichier journal*.

Vous pouvez configurer ce type d'application de gestion des services afin de contrôler les fichiers journaux Data Protector pour des entrées de journal spécifiques (événements Data Protector) et définir une action à effectuer dans le cas où un événement Data Protector particulier est détecté.

Pour plus d'informations sur les fichiers journaux Data Protector, reportez-vous au *Guide de dépannage HP Data Protector* et à l'aide en ligne. Notez qu'aucune spécification de formatage des fichiers journaux n'est fournie.

## Journal de l'application Windows

Certaines applications de gestion des services, telles que le logiciel HP Operations Manager pour Windows (OMW), contrôlent le journal de l'application Windows.

Pour activer le transfert automatique de tous les messages Data Protector et des messages concernant les services Data Protector (s'ils sont arrêtés) vers le journal de l'application Windows, réglez la variable `EventLogMessages` dans le fichier d'options globales Data Protector sur 1. Pour plus d'informations sur le fichier d'options globales Data Protector, reportez-vous au *Guide de dépannage HP Data Protector*.

## Rapports Java en ligne

Data Protector offre une fonction de création de rapports Java en ligne permettant de configurer, d'exécuter et d'imprimer tous les rapports intégrés de Data Protector, en temps réel et de façon interactive. Pendant la génération de rapports Java, la fonctionnalité Data Protector correspondante accède directement au Gestionnaire de cellule pour extraire les données en cours. Vous pouvez mettre à disposition cet applet Java via un serveur Web, le copier sur la machine client pour un accès direct ou l'utiliser en local. Pour utiliser cette fonction, seul un navigateur Web pris en charge est nécessaire. L'installation de l'interface de Data Protector sur le système n'est pas utile. Vous pouvez utiliser la fonction de génération de rapports Java non seulement pour accéder directement à vos rapports en ligne, mais aussi pour reconfigurer la structure (ajouter de nouveaux rapports à un programme ou modifier les paramètres d'un rapport, par exemple).

## Mécanisme de vérification et de maintenance Data Protector

Data Protector offre un puissant mécanisme d'auto-vérification et de maintenance, lequel intervient quotidiennement pour améliorer la fiabilité et la prévisibilité opérationnelles du système. Les tâches d'auto-vérification et de maintenance de Data Protector sont notamment les suivantes :

- Supports libres insuffisants
- Expiration de la licence Data Protector

Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "vérifications effectuées par Data Protector".

## Gestion centralisée, environnement distribué

Grâce au MoM Data Protector, les administrateurs peuvent gérer de façon centralisée un environnement d'entreprise composé de plusieurs systèmes Gestionnaire de cellule Data Protector. L'administrateur du système MoM effectue depuis une seule console toutes les tâches de configuration, de gestion des supports, de contrôle et de génération de rapports d'état pour l'ensemble de l'entreprise. Ainsi, la gestion de nombreux systèmes Gestionnaire de cellule Data Protector s'avère tout aussi simple que celle d'un système unique. Les fournisseurs de services informatiques peuvent gérer les grands environnements de leurs clients sans besoin de personnel supplémentaire. Pour plus d'informations sur le système MoM, recherchez l'entrée suivante dans l'index de l'aide en ligne : "environnement MoM".

## Utilisation des données fournies par Data Protector

### Exemples d'utilisation des données

Voici quelques exemples illustrant ce qu'il est possible de faire avec les données fournies par Data Protector :

- Envoi régulier de rapports par e-mail aux opérateurs de sauvegarde, aux utilisateurs finaux et aux responsables de l'entreprise (fonction de génération de rapports intégrée de Data Protector permettant l'envoi d'e-mail).
- Rapports de sauvegarde créés sur un serveur Web pour les rendre accessibles sur demande (fonction de génération de rapports intégrée de Data Protector permettant l'enregistrement au format HTML).
- Envoi d'événements Data Protector majeurs et critiques vers votre solution d'administration réseau, telle que HP Network Node Manager (moteur de notification intégré de Data Protector permettant l'envoi d'interruptions SNMP).

---

# 7 Fonctionnement de Data Protector

## Dans ce chapitre

Ce chapitre décrit le fonctionnement de Data Protector. Il explique les processus (sous UNIX) et les services (sous Windows) Data Protector, ainsi que les sessions de sauvegarde, de restauration et de gestion des supports.

Il s'organise comme suit :

“Processus ou services Data Protector” à la page 237

“Sessions de sauvegarde” à la page 239

“Sessions de restauration” à la page 245

“Session de copie d'objet” à la page 249

“Sessions de consolidation d'objet” à la page 253

“Sessions de vérification d'objet” à la page 256

“Sessions de gestion des supports” à la page 258

## Processus ou services Data Protector

Data Protector exécute en arrière-plan différents processus (sous UNIX) et services (sous Windows) qui lui permettent de lancer les sessions de sauvegarde et de restauration. Il fournit les voies de communication nécessaires, active les sessions de sauvegarde et de restauration, lance les Agents de disque et les Agents de support, enregistre les informations concernant les éléments sauvegardés, gère les supports et exécute d'autres fonctions similaires.

Inet

Le service Inet Data Protector s'exécute sur chaque système Windows de la cellule Data Protector. Inet est responsable de la communication entre les systèmes de la cellule et lance les processus requis pour les sauvegardes et les restaurations. Le service Inet Data Protector est lancé dès que Data Protector

est installé sur un système. Sur les systèmes UNIX, le démon inet système (INETD) lance le processus Inet Data Protector.

CRS	Le processus (service) CRS (Cell Request Server) s'exécute sur le Gestionnaire de cellule Data Protector. Il lance et contrôle les sessions de sauvegarde et de restauration. Le service est lancé dès que Data Protector est installé sur le système Gestionnaire de cellule. Il est relancé à chaque redémarrage du système.
KMS	Le processus (service) du serveur gestionnaire de clés (KMS - Key Management Server) s'exécute sur le Gestionnaire de cellule et assure la gestion des clés pour la fonctionnalité de cryptage Data Protector. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.
MMD	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 liées aux périphériques et à la gestion des supports. Il est lancé par le processus (service) CRS.
RDS	Le processus RDS (Raima Database Server, serveur de base de données Raima) 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.
UIProxy	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.

Pour savoir comment lancer ou arrêter manuellement les processus et services de Data Protector, reportez-vous à l'aide en ligne.

# Sessions de sauvegarde

Cette section explique comment lancer une session de sauvegarde et décrit le déroulement d'une session de ce type, ainsi que les processus et services impliqués.

## Qu'est-ce qu'une session de sauvegarde ?

Dès qu'une spécification de sauvegarde est lancée, elle devient une session de sauvegarde. Au cours d'une session de sauvegarde, les données d'une source, généralement un disque dur, sont copiées vers une destination, généralement un support à bande. Le résultat d'une session de sauvegarde est une copie de données sur un jeu de supports de sauvegarde.

## Sessions de sauvegarde interactives ou planifiées

### Sessions de sauvegarde planifiées

Une session de sauvegarde planifiée est lancée par le planificateur Data Protector à l'heure spécifiée. Vous pouvez suivre l'évolution de la session dans le moniteur Data Protector.

### Session de sauvegarde interactive

Une session de sauvegarde interactive est lancée directement depuis l'interface utilisateur Data Protector. Le moniteur Data Protector démarre immédiatement et vous pouvez alors suivre l'évolution de la session de sauvegarde. Notez que plusieurs utilisateurs peuvent suivre une même session de sauvegarde. Vous pouvez arrêter le contrôle en déconnectant l'interface utilisateur de la session. La session continuera alors en arrière-plan.

## Flux de données et processus d'une session de sauvegarde

### Déroulement d'une session de sauvegarde

Le flux de données d'une session de sauvegarde est présenté dans la [Figure 60](#) à la page 241. Notez que le flux de données et les processus décrits dans cette section sont ceux d'une session de sauvegarde réseau standard. Pour une présentation du flux de données et des processus propres à d'autres types de sauvegarde, tels que les sauvegardes Split Mirror, reportez-vous aux chapitres correspondants.

Au démarrage d'une session de sauvegarde, les événements suivants se produisent :

1. Le processus processus BSM (Backup Session Manager, gestionnaire de session de sauvegarde) est lancé sur le système Gestionnaire de cellule et contrôle la session de sauvegarde. Il lit la spécification de sauvegarde pour déterminer les éléments à sauvegarder, ainsi que les options, les supports et les périphériques à utiliser pour la sauvegarde.
2. Le BSM (Backup Session Manager, gestionnaire de session de sauvegarde) ouvre la base de données IDB et y écrit les informations concernant la session de sauvegarde : messages générés, informations concernant les données sauvegardées, périphériques et supports utilisés pour la session.
3. Le BSM lance des Agents de support sur les systèmes associés aux périphériques configurés pour la sauvegarde. Un Agent de support est lancé pour chaque lecteur utilisé en parallèle. Le nombre d'Agents de support pouvant être lancés dans la cellule est limité par la configuration de la cellule et par le nombre de licences que vous avez achetées.

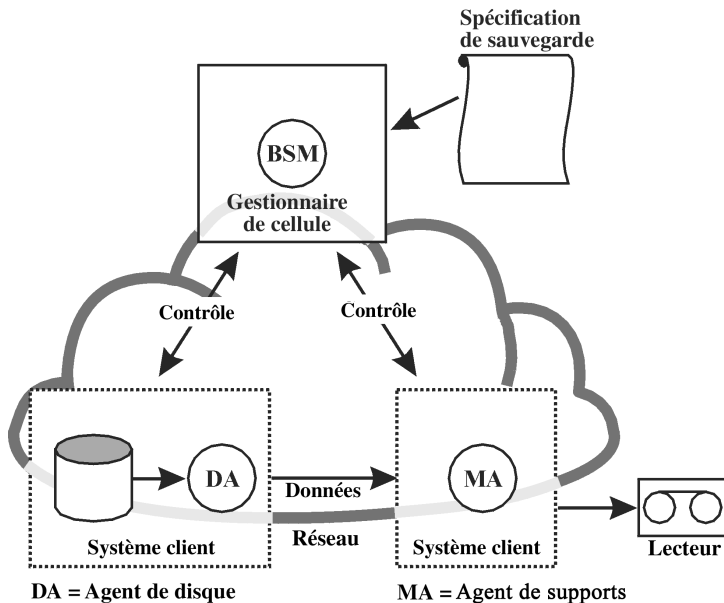
Dans une session de sauvegarde avec mise en miroir d'objet, le gestionnaire BSM lance également les Agents de support qui seront utilisés pour la mise en miroir.

4. Le BSM lance un Agent de disque pour chaque disque à sauvegarder en parallèle. Le nombre effectif d'Agents de disque qu'il est possible de lancer dépend de la simultanéité des Agents de disque, telle qu'elle a été définie au niveau de la spécification de sauvegarde. La simultanéité correspond au nombre d'Agents de disque pouvant être lancés simultanément de sorte que les données soient envoyées en parallèle à un Agent de support et que le périphérique puisse fonctionner en mode continu.
5. Les Agents de disque lisent les données des disques et les transmettent aux Agents de support qui les écrivent sur des supports.

Dans une session de sauvegarde avec mise en miroir d'objet, les Agents de support utilisés pour l'écriture des objets mis en miroir forment une chaîne. Chaque Agent de support écrit les données reçues sur le support et les transmet à l'Agent de support suivant dans la chaîne.

6. Le BSM contrôle l'avancement de la session et lance des Agents de disque et des Agents de support supplémentaires en fonction des besoins.
7. Enfin, le BSM ferme la session lorsqu'elle est terminée.





**Figure 60 Flux de données de la session de sauvegarde (1)**

### Nombre de sessions pouvant être lancées simultanément

Un certain nombre de sessions de sauvegarde peuvent être lancées simultanément dans la cellule. Ce nombre dépend des ressources de la cellule, notamment de la disponibilité des périphériques et de la configuration du Gestionnaire de cellule : vitesse du processeur, taille de la mémoire principale et autres paramètres similaires. Pour éviter que les processus de Data Protector ne dépassent les capacités du système, le nombre maximum de sessions de sauvegarde simultanées est limité. Il est possible de configurer cette limite.

La [Figure 61](#) à la page 242 présente plusieurs sessions exécutées simultanément.

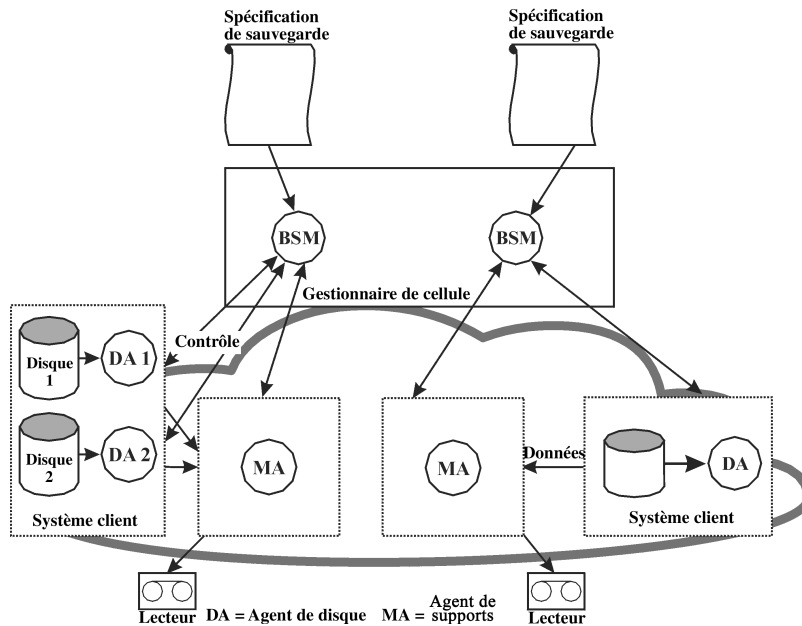


Figure 61 Flux de données d'une session de sauvegarde - sessions multiples

## Commandes pré-exécution et post-exécution

Les commandes Data Protector pré-exécution permettent d'effectuer certaines opérations avant qu'une session de sauvegarde ou de restauration ne commence. Les commandes Data Protector post-exécution permettent d'effectuer certaines opérations au terme d'une session de sauvegarde ou de restauration. Exemple d'opération pré-exécution type : fermer la base de données pour mettre les données dans un état cohérent.

Les commandes pré-exécution et post-exécution peuvent être soit définies pour une spécification de sauvegarde et, à ce titre, exécutées sur le système Gestionnaire de cellule, soit définies comme option d'objet sauvegarde, et donc exécutées sur le système client sur lequel l'Agent de disque correspondant a été lancé.

Les commandes pré-exécution et post-exécution peuvent être écrites sous forme de fichiers exécutables ou de scripts shell. Elles ne sont pas fournies par Data Protector et doivent être écrites séparément, par exemple par l'opérateur de sauvegarde.

## Mise en attente des sessions de sauvegarde

### Délai d'attente

Au démarrage d'une session de sauvegarde, Data Protector tente d'allouer toutes les ressources nécessaires, telles que les périphériques. La session est mise en attente jusqu'à ce que les ressources minimales requises soient disponibles. Si les ressources ne sont toujours pas disponibles au terme du délai d'attente, la session est abandonnée. Le délai d'attente peut être défini à l'aide de l'option globale `SmWaitForDevice`.

### Optimisation de la charge

Pour optimiser la charge du système Gestionnaire de cellule, Data Protector peut lancer un certain nombre de sessions de sauvegarde en même temps. Ce nombre est égal à 5 par défaut et peut être modifié au niveau du fichier d'options globales. Si le nombre de sessions planifiées devant être lancées simultanément est supérieur au nombre par défaut, les sessions supplémentaires sont mises en file d'attente et lancées une fois les autres terminées.

## Demandes de montage au cours d'une session de sauvegarde

### Qu'est-ce qu'une demande de montage ?

Une demande de montage apparaît au cours d'une session de sauvegarde lorsque Data Protector requiert un autre support pour effectuer la sauvegarde et que celui-ci n'est pas disponible.

Data Protector peut émettre une demande de montage pour l'un des motifs suivants :

### Emission d'une demande de montage

- L'espace du support de sauvegarde est insuffisant et aucun support supplémentaire n'est disponible.
- La stratégie d'allocation de supports Data Protector définie requiert un support qui n'est pas présent dans le périphérique.
- Les supports utilisés pour la sauvegarde ne sont pas disponibles dans l'ordre défini au niveau de la liste de préallocation.

Pour plus d'informations, reportez-vous à la section "[Ajout de données aux supports pendant des sessions de sauvegarde](#)" à la page 163 et à la section "[Sélection des supports utilisés pour la sauvegarde](#)" à la page 163.

## Réponse à une demande de montage

Répondre à une demande de montage consiste à fournir les supports requis et à demander à Data Protector de continuer la sauvegarde.

Data Protector vous permet de définir les opérations à effectuer en cas d'émission d'une demande de montage :

### Envoi d'une notification à un opérateur

Vous pouvez configurer une notification Data Protector pour que l'opérateur reçoive un e-mail contenant les informations relatives à la demande de montage. L'opérateur peut dans ce cas prendre les mesures appropriées, par exemple charger manuellement le support requis ou abandonner la session. Pour plus de détails, reportez-vous à la section "[Génération de rapports et notification](#)" à la page 232.

### Automatisation d'une demande de montage

Vous pouvez configurer des opérations automatisées destinées à traiter les demandes de montage. Pour cela, rédigez un script ou un programme de commandes permettant d'effectuer les actions souhaitées.

## Sauvegarde en mode détection de disques

### Qu'est-ce que la détection de disques ?

Lors d'une sauvegarde en mode détection de disques, Data Protector crée une liste détaillée des disques présents sur le système cible une fois la session de sauvegarde lancée, et sauvegarde tous ces disques. Ainsi, tous les disques locaux présents sur le système sont sauvegardés, même s'ils ne figuraient pas sur le système au moment de la configuration de la sauvegarde. La sauvegarde en mode détection de disques est particulièrement utile dans les environnements dynamiques dont les configurations changent rapidement. Elle permet de sélectionner ou d'exclure des répertoires spécifiques dans la sauvegarde.

### Comparaison avec une sauvegarde standard

Dans le cas d'une sauvegarde standard, vous configurez la sauvegarde en définissant explicitement des disques, des répertoires et d'autres objets spécifiques dans la spécification de sauvegarde. Ces objets sont les seuls sauvegardés. Si vous ajoutez des disques au système ou si vous souhaitez sauvegarder d'autres objets, vous devez modifier manuellement la spécification de sauvegarde ainsi que les nouveaux objets. Lorsque vous configurez la sauvegarde, vous pouvez sélectionner la méthode à utiliser : sauvegarde en mode détection de disques ou standard.

# Sessions de restauration

Cette section explique comment lancer une session de restauration et décrit le déroulement d'une session de ce type, ainsi que les processus et services impliqués.

## Qu'est-ce qu'une session de restauration ?

Lors d'une session de restauration, Data Protector extrait les données d'une copie de sauvegarde, généralement un support à bande, pour les transférer sur un disque.

Une session de restauration est lancée de manière interactive. Vous devez tout d'abord indiquer à Data Protector les éléments à restaurer. Les supports requis sont ensuite automatiquement sélectionnés. Enfin, vous devez définir certaines options et lancer la restauration. L'avancement de la session peut être suivi par la personne ayant lancé la session, mais aussi par d'autres utilisateurs.

## Flux de données et processus d'une session de restauration

### Déroulement d'une session de restauration

Lorsqu'une session de restauration est lancée, comme illustré à la [Figure 62](#) à la page 246, les événements suivants se produisent :

1. Gestionnaire de session de restauration Le processus RSM (Restore Session Manager, gestionnaire de session de restauration) est lancé sur le système Gestionnaire de cellule. Ce processus contrôle la session de restauration.
2. Le RSM ouvre la base de données IDB, lit les données relatives aux supports requis pour la restauration et écrit les informations concernant la session de restauration, par exemple les messages générés.
3. Le RSM lance les Agents de support sur les systèmes associés aux périphériques utilisés pour la restauration. Le RSM lance un Agent de support pour chaque lecteur utilisé en parallèle.
4. Le RSM lance un Agent de disque pour chaque disque restauré en parallèle. Le nombre d'Agents de disque pouvant être lancés simultanément dépend des objets sélectionnés en vue de la restauration. Pour plus de détails, reportez-vous à la section "[Restaurations parallèles](#)" à la page 247.
5. Les Agents de support lisent les données des supports et les transmettent aux Agents de disque qui les écrivent sur des disques. Le RSM contrôle l'avancement de la session et lance des Agents de disque et des Agents de support supplémentaires en fonction des besoins.

6. Le RSM ferme la session lorsqu'elle est terminée.

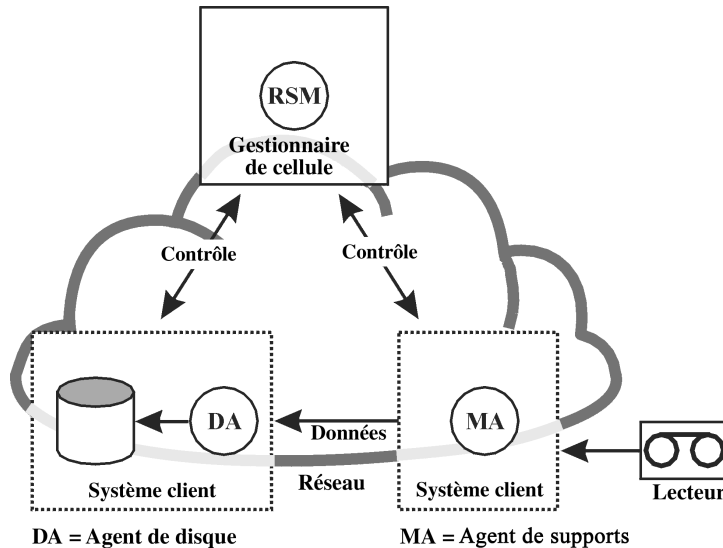


Figure 62 Flux de données d'une session de restauration

### Nombre de sessions pouvant être lancées simultanément

Un certain nombre de sessions peuvent être lancées simultanément dans la cellule. Ce nombre dépend des ressources de la cellule : Gestionnaire de cellule, systèmes associés aux périphériques connectés, etc.

### Mise en attente des sessions de restauration

#### Délai d'attente

Au démarrage d'une session de restauration, Data Protector tente d'allouer toutes les ressources nécessaires, telles que les périphériques. La session reste en file d'attente tant que les ressources minimales requises ne sont pas disponibles. Data Protector tente d'allouer les ressources pendant une période spécifique : le délai d'attente. Vous pouvez configurer ce dernier. Si les ressources ne sont toujours pas disponibles au terme du délai d'attente, la session est abandonnée.

## Demandes de montage au cours d'une session de restauration

### Qu'est-ce qu'une demande de montage ?

Une demande de montage apparaît au cours d'une session de restauration lorsque les supports requis en vue de la restauration ne sont pas disponibles dans le périphérique. Data Protector permet de définir les opérations à effectuer en cas d'émission d'une demande de montage.

### Réponse à une demande de montage

Répondre à une demande de montage consiste à fournir le support requis, ou toute copie du support, et à demander à Data Protector de continuer la restauration.

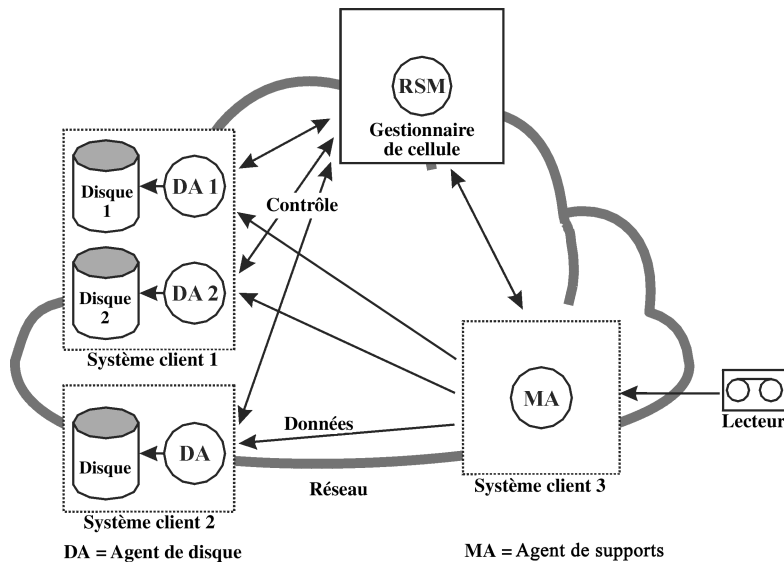
## Restaurations parallèles

### Qu'est-ce qu'une restauration parallèle ?

Lors d'une restauration parallèle, des données entrelacées issues de différents objets sont lues simultanément à partir d'un support, selon un chemin unique, puis sont restaurées. La restauration parallèle améliore les performances de façon significative lorsqu'il s'agit de restaurer plusieurs objets à partir du même support. Pour plus de détails, reportez-vous à la [Figure 63](#) à la page 248.

### Comparaison avec une sauvegarde standard

Les données de plusieurs Agents de disque sont (la plupart du temps) multiplexées et stockées sur le support. Reportez-vous à la [Figure 43](#) à la page 164. Lors d'une restauration standard, Data Protector lit les données multiplexées sur le support et ne rassemble que les parties requises pour l'objet sélectionné. Lors de la restauration de l'objet suivant, Data Protector doit rembobiner le support et lire les parties correspondant à cet autre objet, en supposant que les deux objets se trouvent sur le même support et ont été écrits par multiplexage.



**Figure 63 Flux de session d'une restauration parallèle**

Lors d'une restauration parallèle, Data Protector lit les données multiplexées pour tous les objets sélectionnés et rassemble à la volée les parties requises pour chacun d'entre eux, en transmettant les données aux Agents de disque appropriés. Les performances en termes de lecture du support sont ainsi améliorées. Les performances en terme d'écriture sur disques sont également optimisées si les objets sélectionnés doivent être écrits sur plusieurs disques physiques différents : dans ce cas, les données sont copiées sur plusieurs disques en même temps.

## Restauration multiple et rapide de fichier unique

Data Protector utilise la fonctionnalité de restauration d'objets non contigus pour améliorer les performances de restauration. Après avoir restauré un fichier ou une arborescence, Data Protector se repositionne directement au niveau de l'arborescence ou du fichier suivant sur le support, si les fichiers ou les arborescences sont séparés au minimum par un segment, et continue la restauration.

Vous pouvez lancer plusieurs Agents de disque pour un objet restauration individuel. De cette manière, la restauration de plusieurs fichiers individuels situés à différents emplacements du support est beaucoup plus rapide que si Data Protector devait parcourir ce dernier.



## Reprise des sessions de restauration

Les sessions de restauration qui n'ont pas été correctement réalisées (en raison d'un problème de réseau par exemple) peuvent être reprises via la fonctionnalité de reprise de session Data Protector. Lorsque vous reprenez une session qui a échoué, Data Protector poursuit la restauration dans une nouvelle session à partir du point où la session qui a échoué s'est interrompue.

## Session de copie d'objet

Cette section explique comment lancer une session de copie et décrit le déroulement d'une session de ce type, ainsi que les processus et services impliqués.

### Qu'est-ce qu'une session de copie d'objet ?

Une session de copie d'objets est un processus qui consiste à créer une copie supplémentaire des données sauvegardées, copiées ou consolidées sur un jeu de supports distinct. Au cours d'une session de copie, les objets sauvegardés, copiés ou consolidés qui sont sélectionnés sont copiés du support source vers le support cible.

## Sessions de copie d'objet automatique et interactive

### Session de copie d'objet automatique

Une session automatique de copie d'objet peut être planifiée ou lancée immédiatement après une sauvegarde, une copie ou une consolidation d'objet. Une session planifiée de copie d'objet démarre à l'heure que vous avez spécifiée à l'aide du planificateur Data Protector. Une session de copie d'objet après sauvegarde, copie ou consolidation débute une fois la session spécifiée terminée. Vous pouvez suivre l'évolution de la session de copie d'objet automatique dans le moniteur Data Protector.

### Session de copie d'objet interactive

Une session de copie d'objet interactive est lancée directement depuis l'interface utilisateur Data Protector. Le moniteur Data Protector démarre immédiatement et vous pouvez alors suivre l'évolution de la session. Plusieurs utilisateurs peuvent contrôler la même session de copie d'objet. Vous pouvez arrêter le contrôle en déconnectant l'interface utilisateur de la session. La session continuera alors en arrière-plan.

## Flux de données et processus d'une session de copie d'objet

### Déroulement d'une session de copie d'objet

Le flux d'informations d'une session de copie d'objet est présenté dans la [Figure 64](#) à la page 252. Au démarrage d'une session de copie d'objet, les événements suivants se produisent :

1. Le processus CSM (Copy and Consolidation Session Manager, gestionnaire de session de copie et de consolidation) est lancé sur le système Gestionnaire de cellule. Ce processus lit les spécifications de copie d'objet en recherchant les informations relatives aux objets qui doivent être copiés ainsi qu'aux options, supports et périphériques à utiliser. Il contrôle également la session de copie d'objet.
2. Le CSM ouvre la base de données IDB, lit les données relatives aux supports requis pour la copie et écrit les informations concernant la session de copie d'objet, par exemple les messages générés.
3. Le processus CSM verrouille les périphériques. La session est mise en attente jusqu'à ce que tous les Agents de support de lecture et les Agents de support d'écriture requis soient verrouillés, le délai d'attente étant le même que pour la sauvegarde. Si les ressources ne sont toujours pas disponibles au terme du délai d'attente, la session est abandonnée.
4. Le CSM lance les Agents de support sur les systèmes possédant des périphériques configurés pour la copie. Les Agents de support chargent les supports sources et cibles alloués en fonction des stratégies de sauvegarde.
5. Les Agents de support lisent les données dans les supports sources et se connectent aux Agents de support porteurs des supports cibles.

Si les périphériques de destination ne sont pas spécifiés par objet, Data Protector les sélectionne automatiquement parmi ceux que vous avez choisis dans la spécification de copie d'objet, en fonction des critères suivants et par ordre de priorité :

- Les périphériques de destination ayant la même taille de bloc que les périphériques sources sont sélectionnés avant ceux dont la taille de bloc diffère.
- Les périphériques connectés localement sont sélectionnés avant les périphériques en réseau.

6. Les Agents de support porteurs des supports cibles acceptent les connexions provenant des Agents de support porteurs des supports sources et commencent à écrire les copies d'objet sur les supports cibles.

Si la taille de bloc du périphérique source est inférieure à la taille de bloc du périphérique de destination, les blocs sont redimensionnés à ce stade de la session de copie d'objet.

7. Pour tous les objets copiés, le CSM met à jour les entrées de protection IDB selon les options spécifiées pour la session de copie.

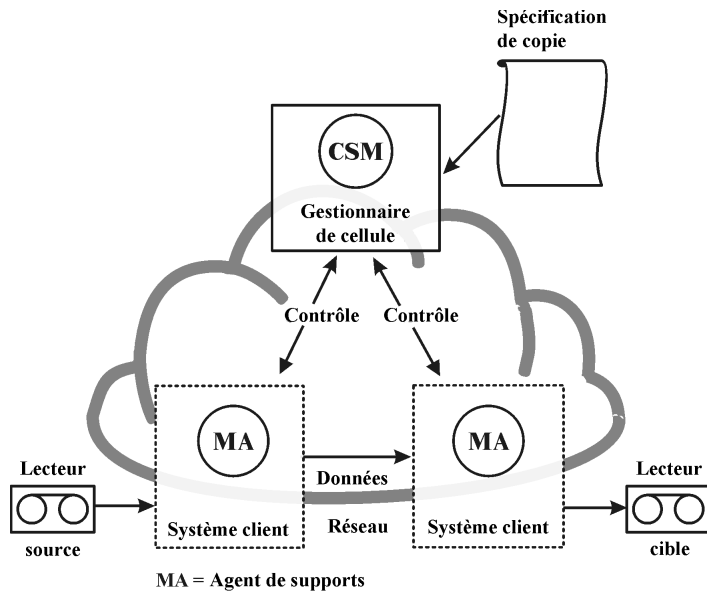
La protection des objets sources ayant échoué est également mise à jour afin de permettre le recyclage si l'option de recyclage a été spécifiée pour la session.

8. Le CSM ferme la session de copie d'objet lorsqu'elle est terminée.

### Nombre de sessions pouvant être lancées simultanément

Un certain nombre de sessions de copie d'objet peuvent s'exécuter simultanément dans la cellule. Ce nombre dépend des ressources de la cellule : Gestionnaire de cellule et les systèmes associés aux périphériques connectés.

Cependant, il n'est pas possible d'exécuter plusieurs sessions de copie d'objet en parallèle à partir de la même spécification de copie d'objet.



**Figure 64 Flux de données d'une session de copie d'objet**

## Mise en attente des sessions de copie d'objet

### Délai d'attente

Lorsqu'une session de copie d'objet débute, Data Protector essaie d'allouer toutes les ressources nécessaires. La session est mise en attente jusqu'à ce que les ressources minimales requises soient disponibles. Si les ressources ne sont toujours pas disponibles au terme du délai d'attente, la session est abandonnée. Le délai d'attente peut être défini à l'aide de l'option globale `SmWaitForDevice`.

## Demands de montage dans une session de copie d'objet

### Qu'est-ce qu'une demande de montage ?

Une demande de montage dans une session de copie d'objet est émise lorsqu'un support source ou cible nécessaire pour l'opération de copie d'objet n'est pas disponible.

## Réponse à une demande de montage

La réponse à une demande de montage inclut la fourniture du support requis et la confirmation de la demande de montage. Si le support source requis dispose de copies de supports, vous pouvez fournir une copie à la place du support d'origine.

# Sessions de consolidation d'objet

Cette section explique comment lancer une session de consolidation d'objet et décrit le déroulement d'une session de ce type, ainsi que les processus et services impliqués.

## Qu'est-ce qu'une session de consolidation d'objet ?

Une session de consolidation d'objet est un processus permettant de fusionner une chaîne de restauration d'un objet sauvegarde, comprenant une sauvegarde complète et au moins une sauvegarde incrémentale, en une nouvelle version consolidée de cet objet. Pendant la session de consolidation d'objet, Data Protector lit les données sauvegardées à partir du support source, les transfère et écrit la version consolidée sur le support cible.

Pour plus de détails, reportez-vous au [Chapitre 10](#) à la page 275.

## Sessions de consolidation d'objet automatique et interactive

### Session de consolidation d'objet automatique

Une session de consolidation d'objet automatique peut être planifiée ou lancée immédiatement après une sauvegarde. Une session planifiée de consolidation d'objet démarre à l'heure que vous avez spécifiée à l'aide du planificateur Data Protector. Une session de consolidation d'objet après sauvegarde débute une fois la session de sauvegarde spécifiée terminée. Vous pouvez suivre l'évolution d'une session de consolidation d'objet automatique dans le moniteur Data Protector.

### Session de consolidation d'objet interactive

Une session de consolidation d'objet interactive est lancée directement depuis l'interface utilisateur de Data Protector. Le moniteur Data Protector démarre immédiatement et vous pouvez alors suivre l'évolution de la session. Plusieurs utilisateurs peuvent contrôler la même session de consolidation d'objet. Vous pouvez arrêter le contrôle en déconnectant l'interface utilisateur de la session. La session continuera alors en arrière-plan.

## Flux de données et processus d'une session de consolidation d'objet

Au démarrage d'une session de consolidation d'objet, les événements suivants se produisent :

1. Le processus CSM (Copy and Consolidation Session Manager, gestionnaire de session de copie et de consolidation) est lancé sur le système Gestionnaire de cellule. Ce processus lit les spécifications de consolidation d'objet en recherchant les informations relatives aux objets qui doivent être consolidés ainsi qu'aux options, supports et périphériques à utiliser. Il contrôle également la session de consolidation d'objet.
2. Le CSM ouvre la base de données IDB, lit les données relatives aux supports requis et écrit les informations concernant la session de consolidation d'objet, par exemple les messages générés.
3. Le processus CSM verrouille les périphériques. La session est mise en attente jusqu'à ce que tous les Agents de support de lecture et les Agents de support d'écriture requis soient verrouillés, le délai d'attente étant le même que pour la sauvegarde. Si les ressources ne sont toujours pas disponibles au terme du délai d'attente, la session est abandonnée.
4. Le CSM lance les Agents de support sur les systèmes possédant des périphériques qui seront utilisés pour la session. Les Agents de support chargent les supports sources et cibles alloués en fonction des stratégies de sauvegarde.

Si les périphériques de destination ne sont pas spécifiés par objet, Data Protector les sélectionne automatiquement parmi ceux que vous avez choisis dans la spécification de consolidation d'objet, en fonction des critères suivants et par ordre de priorité :

- Les périphériques de destination ayant la même taille de bloc que les périphériques sources sont sélectionnés avant ceux dont la taille diffère.
- Les périphériques connectés localement sont sélectionnés avant les périphériques en réseau.

5. Un Agent de support lit la version complète de l'objet. Il envoie les données à un autre Agent de support qui lit les versions incrémentales de l'objet. Cet agent effectue la consolidation proprement dite et envoie les données à l'Agent de support qui écrit les données sur le support cible.

Si la sauvegarde complète et les sauvegardes incrémentales résident dans la même bibliothèque de fichiers, c'est le même Agent de support qui lit toutes les sauvegardes et les consolide.

Si la taille de bloc du périphérique source est inférieure celle du périphérique de destination, les blocs sont redimensionnés.

6. Le CSM ferme la session de consolidation d'objet lorsqu'elle est terminée.

### Nombre de sessions pouvant être lancées simultanément

Un certain nombre de sessions de consolidation d'objet peuvent s'exécuter simultanément dans la cellule. Les sessions de consolidation sont traitées comme des sessions de sauvegarde et leur nombre est limité par les mêmes facteurs.

## Mise en attente des sessions de consolidation d'objet

### Délai d'attente

Lorsqu'une session de consolidation d'objet débute, Data Protector essaie d'allouer toutes les ressources nécessaires. La session est mise en attente jusqu'à ce que les ressources minimales requises soient disponibles. Si les ressources ne sont toujours pas disponibles au terme du délai d'attente, la session est abandonnée. Le délai d'attente peut être défini à l'aide de l'option globale `SmWaitForDevice`.

## Demandes de montage dans une session de consolidation d'objet

### Qu'est-ce qu'une demande de montage ?

Une demande de montage dans une session de consolidation d'objet est émise lorsqu'un support source ou cible nécessaire pour l'opération de consolidation d'objet n'est pas disponible.

### Réponse à une demande de montage

La réponse à une demande de montage inclut la fourniture du support requis et la confirmation de la demande de montage. Si le support source requis dispose de copies de supports, vous pouvez fournir une copie à la place du support d'origine.

# Sessions de vérification d'objet

Cette section explique comment lancer une session de vérification d'objet et décrit le déroulement d'une session de ce type, ainsi que les processus et services impliqués.

## Qu'est-ce qu'une session de vérification d'objet?

Une session de vérification d'objet est un processus au cours duquel les segments de support alloués à un ou plusieurs objets désignés sont vérifiés. Ce processus examine les informations contenues dans les segments d'en-tête et lit les blocs de données dans les segments de données afin de contrôler leur format. Si un contrôle CRC (contrôle de redondance cyclique) a été effectué au cours de la sauvegarde d'origine, il le recalcule également et le compare à l'original.

Data Protector peut effectuer la vérification sur l'hôte source de la sauvegarde. Il contrôle alors les composants de Data Protector présents dans le chemin de restauration. Il peut également l'effectuer sur un hôte distinct et vérifiera alors qu'il est possible d'exécuter une restauration dans un autre emplacement, ou directement sur l'hôte comportant l'Agent de support concerné. Dans ce cas, seules les données sont vérifiées.

## Sessions de vérification d'objet automatiques et interactives

### Session de vérification d'objet automatique

Vous pouvez spécifier l'heure d'exécution d'une session de vérification d'objet automatique à l'aide du planificateur de Data Protector. Vous avez également la possibilité d'exécuter cette session immédiatement à la fin d'une session de sauvegarde, de copie d'objet ou de consolidation d'objet. Vous pouvez suivre l'évolution de ces sessions dans le moniteur Data Protector.

### Session de vérification d'objet interactive

Vous pouvez démarrer une session de vérification d'objet interactive directement à partir de l'interface Data Protector. Le moniteur Data Protector démarre immédiatement et vous pouvez alors suivre l'évolution de la session. Plusieurs utilisateurs peuvent contrôler la même session de vérification d'objet. Si nécessaire, vous pouvez effectuer d'autres opérations dans l'interface utilisateur et laisser la session se poursuivre à l'arrière-plan.



# Flux de données et processus d'une session de vérification d'objet

## Déroulement d'une session de vérification d'objet

Lorsqu'une session de vérification d'objet démarre, le flux de processus habituel est le suivant :

1. Le processus RSM (Restore Session Manager, gestionnaire de session de restauration) est lancé sur le Gestionnaire de cellule. Il est déclenché par :
  - le planificateur Data Protector, s'il s'agit d'une session planifiée
  - l'événement "fin de session", dans le cas de session post-sauvegarde
  - l'utilisateur (à partir de l'interface utilisateur ou de l'interface de ligne de commande) dans les sessions interactives

Ce processus contrôle la session de vérification.

2. Le RSM ouvre la base de données IDB, lit les données relatives aux objets à vérifier et écrit les informations concernant la session de vérification, par exemple les messages générés.
3. Le RSM lance les Agents de support sur les systèmes sources concernés par la vérification. Le RSM lance un Agent de support pour chaque lecteur utilisé en parallèle.
4. La vérification des données est effectuée par les Agents de disque sur les hôtes de destination. Par conséquent, le RSM lance un Agent de disque pour chaque disque de destination en parallèle. Le nombre d'Agents de disque pouvant être lancés simultanément dépend des objets sélectionnés en vue de la vérification. Le processus est similaire au processus de restauration. Pour plus d'informations, reportez-vous à la section "Restaurations parallèles" à la page 228.
5. Les Agents de support lisent les données des objets et les transmettent aux Agents de disque qui effectuent la vérification. Le RSM contrôle l'avancement de la session et lance des Agents de disque et des Agents de support supplémentaires en fonction des besoins.
6. Le RSM ferme la session de vérification d'objet lorsqu'elle est terminée.

## Variations du flux de processus avec la vérification d'objet

Le processus de vérification d'objet émule le processus de restauration à partir du point où la restauration des données est demandée, jusqu'à celui où les données parviennent sur l'hôte de destination. Au-delà de ce point, le processus de vérification

n'écrit aucune donnée et pour les objets d'intégration d'application, il n'existe aucune communication avec l'intégration d'application.

## Sessions de gestion des supports

### Qu'est-ce qu'une session de gestion des supports ?

Il s'agit d'une session servant à exécuter une action sur les supports, comme l'initialisation, l'analyse de contenu, la vérification des données stockées sur les supports et la copie de supports.

### Connexion à la base de données IDB

Les informations relatives à une session de gestion des supports, notamment les messages générés, sont stockées dans la base de données IDB.

### Suivi d'une session de gestion des supports dans le moniteur Data Protector

Il est possible de visualiser une session de gestion des supports dans la fenêtre de contrôle. Si vous fermez l'interface utilisateur de Data Protector, la session se poursuit en arrière-plan.

## Flux de données d'une session de gestion des supports

### Déroulement d'une session de gestion des supports

Lorsqu'une session de gestion des supports est lancée, les événements suivants se produisent :

1. Le processus MSM (Media Session Manager, gestionnaire de session de gestion des supports) est lancé sur le système Gestionnaire de cellule. Ce processus contrôle la session de gestion des supports.
2. Le MSM lance les Agents de support sur le système associé aux périphériques utilisés pour la session de gestion des supports.
3. Les Agents de support exécutent l'opération demandée et envoient les messages générés à l'interface utilisateur Data Protector, celle-ci permettant de suivre l'évolution de la session. La session est également stockée dans la base de données IDB.
4. Le MSM ferme la session lorsqu'elle est terminée.

## Nombre de sessions pouvant être lancées simultanément

Un certain nombre de sessions de gestion des supports peuvent être exécutées simultanément dans la cellule si ces sessions n'utilisent pas les mêmes ressources (périphériques, supports, etc.).



---

# 8 Intégration avec des applications

Ce chapitre fournit une brève description de l'intégration de Data Protector avec des applications de base de données telles que Microsoft Exchange Server, Oracle Server, IBM DB2 UDB et Informix Server, ainsi qu'avec des environnements de virtualisation tels que l'infrastructure virtuelle VMware et Hyper-V.

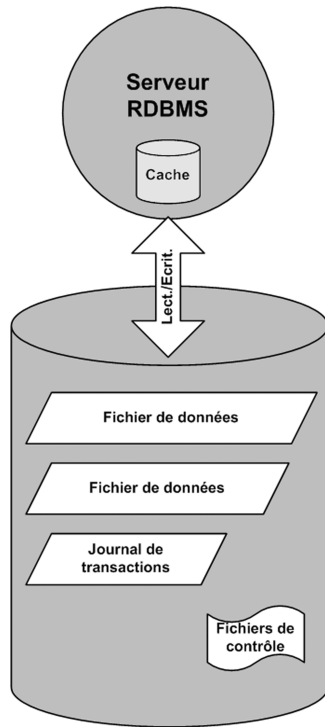
## Intégration aux applications de base de données

Cette section fournit une brève description de l'intégration de Data Protector avec des applications de base de données. Pour obtenir la liste détaillée des applications prises en charge, consultez les dernières matrices de support à l'adresse <http://www.hp.com/support/manuals>.

### Présentation d'une base de données

Du point de vue de l'utilisateur, une **base de données** est un ensemble de données. Les données d'une base sont stockées dans des **tables**. Les tables relationnelles sont définies par leurs colonnes ; un nom leur est attribué. Les données sont enregistrées dans les lignes de la table. Les tables peuvent être reliées entre elles et la base de données peut être utilisée pour mettre en application ces liaisons. Les données peuvent donc être enregistrées dans un **format relationnel** ou sous des structures **orientées objet** comme les méthodes et les types de données abstraits. Les objets peuvent être reliés à d'autres objets et contenir d'autres objets. Une base de données est généralement gérée par le processus serveur (gestionnaire), qui maintient l'intégrité et la cohérence des données.

Que vous utilisiez les structures relationnelles ou celles orientées objet, les données d'une base sont stockées dans des **fichiers**. En interne, il s'agit de structures de base de données qui établissent un mappage logique entre des données et des fichiers, permettant de stocker séparément des types de données différents. On appelle ces divisions logiques des **espaces de table** dans Oracle, des **dbspaces** dans Informix Server et des **segments** dans Sybase.



**Figure 65 Base de données relationnelle**

La [Figure 65](#) à la page 262 présente une base de données relationnelle type qui comporte les structures décrites ci-dessous.

Les **fichiers de données** contiennent physiquement l'ensemble des données d'une base de données. Ils changent de manière aléatoire et peuvent être très volumineux. Un fichier de données est divisé en pages.

Dans les **journaux de transactions**, toutes les transactions des bases de données sont enregistrées avant la suite de leur traitement. Si un échec empêche l'écriture définitive de données modifiées dans un fichier de données, les modifications peuvent être obtenues à partir d'un fichier journal. La récupération, quelle qu'elle soit, s'effectue en deux étapes : la phase "**roll forward**", au cours de laquelle les modifications des transactions sont appliquées dans la base de données principale, et la phase "**roll back**", durant laquelle les transactions non validées sont supprimées.

Les **fichiers de contrôle** contiennent des informations sur la structure physique des bases de données, comme leur nom, les noms et emplacements de leurs fichiers de données et fichiers journaux, ainsi que l'horodatage de leur création. Ces données de contrôle sont conservées dans les fichiers de contrôle, lesquels sont essentiels au bon fonctionnement de la base de données.

La **mémoire cache** du processus serveur de base de données contient les pages les plus fréquemment utilisées des fichiers de données.

La procédure suivante représente le flux standard du traitement d'une transaction :

1. Une transaction est d'abord enregistrée dans le journal de transactions.
2. Les modifications requises dans la transaction sont ensuite appliquées aux pages mises en cache.
3. De temps à autre, des groupes de pages modifiées sont transférés dans des fichiers de données se trouvant sur le disque.

## Sauvegarde de systèmes de fichiers de bases de données et d'applications

Les bases de données changent constamment lorsqu'elles sont connectées. Un serveur de base de données est constitué de plusieurs composants, lesquels permettent de réduire le temps de réponse aux utilisateurs connectés et d'améliorer les performances. Certaines données sont conservées dans la mémoire cache interne, et d'autres dans des fichiers journaux temporaires qui sont transférés à des **points de contrôle**.

Les données d'une base pouvant changer au cours d'une sauvegarde, une sauvegarde de système de fichiers de base de données n'a pas de sens si le serveur de base de données n'est pas mis dans un mode spécial ou même hors ligne. Les fichiers de bases de données enregistrés doivent se trouver dans un état cohérent, sinon les données sont inutilisables.

Il est nécessaire de respecter la procédure suivante pour configurer la sauvegarde d'un système de fichiers de base de données ou d'application :

- Identifiez tous les fichiers de données.
- Préparez deux programmes, l'un capable de fermer la base de données, l'autre de l'ouvrir.
- Configurez la **spécification de sauvegarde** du système de fichiers avec tous ses fichiers de données, puis indiquez le programme de fermeture comme étant une **commande pré-exécution** et le programme d'ouverture comme étant une **commande post-exécution**.

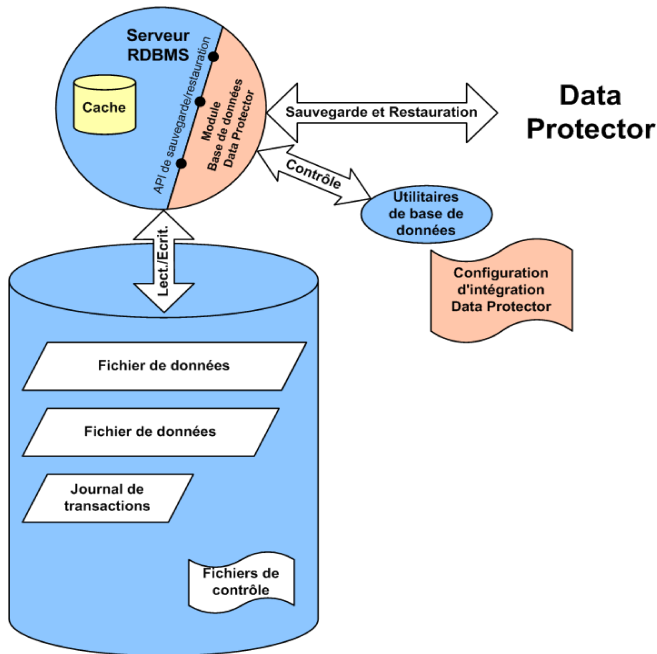
Cette méthode est assez simple à comprendre et à appliquer, mais possède un inconvénient majeur : *la base de données n'est pas accessible pendant la sauvegarde*, ce qui est inacceptable pour la plupart des environnements professionnels.

## Sauvegarde en ligne de bases de données et d'applications

Pour pallier la nécessité de fermer la base de données pendant une sauvegarde, les fournisseurs de bases de données ont mis au point des interfaces permettant de mettre provisoirement la base de données dans un mode spécial afin d'enregistrer les données sur bandes. Les applications serveur restent donc connectées et accessibles par les utilisateurs durant le processus de sauvegarde ou de restauration. Grâce à ces interfaces spécifiques aux applications, il est possible de sauvegarder ou de restaurer des unités logiques de l'application de base de données à l'aide de produits de sauvegarde tels que Data Protector. Les fonctionnalités des API de sauvegarde varient selon les fournisseurs de base de données. Les principales bases de données et applications s'intègrent à Data Protector. Pour connaître la liste détaillée des intégrations prises en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

L'interface de sauvegarde a pour fonction de fournir des données cohérentes (même si elles ne le sont pas sur disque) à l'application de sauvegarde, tout en laissant la base de données opérationnelle.





**Figure 66 Intégration de Data Protector à des bases de données**

La [Figure 66](#) à la page 265 montre comment une base de données relationnelle est intégrée à Data Protector. Data Protector dispose d'une **bibliothèque de base de données** qui est reliée au serveur de base de données. Le serveur de base de données envoie et demande des données à Data Protector. Les utilitaires de base de données sont utilisés pour déclencher les opérations de sauvegarde et de restauration.

Les étapes suivantes constituent une procédure standard pour configurer la sauvegarde d'une base de données avec l'intégration de Data Protector :

1. Un agent spécifique de base de données/d'application est installé sur le système de base de données.
2. L'intégration de Data Protector est configurée pour chaque base de données. Les données nécessaires à Data Protector pour travailler avec cette base de données sont stockées dans le système de base de données (dans des entrées de registre ou des fichiers de configuration). En général, il s'agit notamment de chemins d'accès et de noms/mots de passe d'utilisateurs.
3. La spécification de sauvegarde est préparée à l'aide de l'interface utilisateur de Data Protector.

La base de données reste **en ligne** sans interruption, ce qui constitue un avantage considérable ; en outre, l'utilisation de l'intégration de Data Protector à des bases de données présente d'autres avantages :

- Il n'est pas nécessaire de spécifier l'emplacement des fichiers de données. Ces derniers peuvent se trouver sur des disques différents.
- Il est possible d'explorer la structure logique de la base de données. Vous pouvez également sélectionner un seul sous-ensemble de la base de données.
- En cas de sauvegarde, les applications sont informées et contrôlent les éléments sauvegardés.
- Plusieurs modes de sauvegarde sont possibles. Outre les sauvegardes **complètes**, les utilisateurs peuvent sélectionner des sauvegardes **incrémentales** (niveau de bloc), ou uniquement la sauvegarde de fichiers journaux de transactions.
- Plusieurs modes de restauration sont possibles et, après la restauration de fichiers de données, la base de données peut automatiquement restaurer des journaux de transactions et les appliquer selon leur configuration.

## Intégration avec les environnements de virtualisation

Cette section fournit une brève description des intégrations de Data Protector avec des environnements de virtualisation. Pour obtenir la liste détaillée des environnements pris en charge, consultez les dernières matrices de support à l'adresse <http://www.hp.com/support/manuals>.

Pour plus d'informations, reportez-vous au *Guide d'intégration HP Data Protector pour les environnements de virtualisation*.

## Sauvegarde hors ligne du système de fichiers des machines virtuelles

Etant donné que les machines virtuelles changent constamment lorsqu'elles sont en ligne, vous devez les placer dans un mode spécial, voire les arrêter avant de lancer une sauvegarde du système de fichiers.

Les fichiers du disque qui appartiennent à une machine virtuelle doivent se trouver dans un état cohérent ; sinon l'image de sauvegarde créée pour cette machine virtuelle est inutilisable.

Pour configurer la sauvegarde du système de fichiers d'une machine virtuelle, vous devez identifier tous les fichiers de la machine virtuelle, créer deux programmes capables d'arrêter et de démarrer la machine virtuelle, créer une spécification de sauvegarde du système de fichiers incluant tous les fichiers de la machine virtuelle et définir le programme d'arrêt en tant que commande de pré-exécution et le programme de démarrage en tant que programme de post-exécution.

Cette méthode est relativement simple, mais elle a un inconvénient majeur : la machine virtuelle ne peut pas être utilisée activement durant la sauvegarde.

## Sauvegarde en ligne de machines virtuelles

Data Protector peut utiliser les interfaces spécifiques fournies par les environnements de virtualisation afin d'exécuter une sauvegarde des machines virtuelles en cours d'exécution (sauvegarde en ligne). Selon l'environnement de virtualisation, les applications résidant sur les machines virtuelles peuvent également être placées dans un état cohérent avant le démarrage de la sauvegarde.

La machine virtuelle reste en ligne sans interruption, ce qui constitue un avantage considérable ; en outre, l'utilisation des intégrations de Data Protector avec les bases de données présente d'autres avantages :

- Il n'est pas nécessaire de spécifier l'emplacement des fichiers de données.
- Les environnements de virtualisation sont informés de l'opération de sauvegarde et assurent le suivi des éléments sauvegardés.
- Plusieurs modes de sauvegarde sont possibles.
- Plusieurs modes de restauration sont possibles.



---

# 9 Sauvegarde sur disque

## Dans ce chapitre

Ce chapitre présente les concepts associés à la sauvegarde de données sur disque et les technologies permettant de la mettre en application. Il décrit également les configurations de sauvegarde disque-à-disque prises en charge par Data Protector.

Il s'organise comme suit :

“Généralités” à la page 269

“Avantages de la sauvegarde sur disque” à la page 270

“Périphériques sur disque Data Protector” à la page 271

## Généralités

L'industrie requiert des méthodes de sauvegarde et de restauration de données de plus en plus rapides. En outre, il importe de plus en plus que le temps nécessaire à la sauvegarde et à la restauration des données soit réduit au minimum afin de ne pas interrompre le fonctionnement quotidien des applications de l'entreprise.

Au cours d'un jour ouvrable, nombre d'applications et de bases de données ne cessent d'apporter de petites modifications aux fichiers existants ou de générer une grande quantité de fichiers nouveaux contenant des données stratégiques. Ces fichiers doivent être sauvegardés immédiatement pour que les données qu'ils contiennent ne soient pas perdues. Cette condition implique l'utilisation d'un support rapide pouvant stocker des volumes de données importants et fonctionnant de manière ininterrompue.

Le prix des supports de stockage sur disque est devenu plus abordable ces dernières années. Dans le même temps, la capacité de stockage s'est accrue. En conséquence, des disques simples et des baies de disques à faible coût et hautement performants sont désormais disponibles pour le stockage de données.

La sauvegarde sur disque (également appelée sauvegarde disque à disque) prend une importance croissante. Auparavant, le stockage sur bande était la méthode de prédilection pour la sauvegarde et la restauration en raison de son coût et de sa

capacité à satisfaire aux exigences de récupération après sinistre. Aujourd'hui, un nombre croissant d'entreprises complètent leurs solutions de sauvegarde sur bande par des solutions de sauvegarde sur disque plus rapides. Les données sont ainsi sauvegardées et récupérées plus rapidement.

## Avantages de la sauvegarde sur disque

Dans bon nombre de cas, il n'est pas avantageux d'utiliser des périphériques sur disque pour effectuer des sauvegardes. Les périphériques sur disque sont en fait des fichiers spécifiques dans des répertoires spécifiés sur lesquels vous pouvez stocker des données au lieu ou en plus de les stocker sur bande. La liste suivante présente certaines situations dans lesquelles les périphériques sur disque sont particulièrement utiles :

- De nombreuses applications et bases de données génèrent ou modifient en permanence un grand nombre de fichiers contenant des données stratégiques. Dans ces situations, il est nécessaire de sauvegarder régulièrement les fichiers concernés afin de garantir une restauration sans perte de données.

Dans ces environnements, les périphériques à bande doivent fonctionner généralement en mode marche/arrêt car ils ne reçoivent pas un flux continu de données. Le périphérique à bande peut alors limiter l'accès aux fichiers concernés. En outre, la durée de vie du périphérique de sauvegarde peut être considérablement réduite.

Les sauvegardes peuvent également être réalisées sur un périphérique sur disque, ce qui permet de dépasser les limites décrites. Elle peut faire office de solution de sauvegarde à court terme. Si une solution de sauvegarde à long terme est requise, les données contenues dans les périphériques sur disque peuvent être déplacées régulièrement sur une bande afin de libérer l'espace disque. Ce processus est appelé **sauvegarde de disque en plusieurs étapes**.

- Dans les environnements caractérisés par des lecteurs de disque rapides et très performants et des lecteurs de bande lents, vous pouvez réduire la fenêtre de sauvegarde en effectuant tout d'abord une sauvegarde sur les périphériques sur disque et en déplaçant ensuite les données sur une bande.
- L'utilisation de périphériques sur disque pour la sauvegarde vous permet de bénéficier de stratégies de sauvegarde avancées comme la **sauvegarde synthétique**.
- Les périphériques sur disque permettent de restaurer rapidement des données sauvegardées récemment. Par exemple, les données de sauvegarde peuvent être conservées sur un périphérique sur disque pendant 24 heures pour permettre une restauration rapide et pratique.

- Le mécanisme d'un périphérique sur disque est plus rapide que celui d'une bande. Lors de l'utilisation d'un périphérique sur disque, il n'est pas nécessaire de monter et de démonter la bande. Lors de la sauvegarde ou de la restauration d'un petit volume de données, un périphérique sur disque est plus rapide car son temps d'initialisation est bien moins important que celui d'un lecteur de bande. Dans le cas d'un périphérique sur disque, il n'est pas nécessaire de charger ou de décharger les supports, des tâches fastidieuses dans le cas d'une sauvegarde ou d'une restauration de petite taille. Les avantages de l'utilisation d'un périphérique sur disque apparaissent encore plus évidents lorsqu'on effectue une restauration à partir d'une sauvegarde incrémentale.
- La probabilité de rencontrer des problèmes au niveau des supports, tels que des bandes défectueuses ou un montage incorrect de la bande, est quasiment nulle. La disponibilité des configurations de disque RAID garantit la protection des données en cas de dysfonctionnement d'un disque.
- Les frais généraux sont réduits car il n'est pas nécessaire de manipuler les bandes.
- En règle générale, le stockage sur disque devient de moins en moins onéreux, même comparé au stockage sur bande.

## Périphériques sur disque Data Protector

Data Protector est doté des périphériques sur disque suivant :

- Périphérique de fichier autonome
- Périphérique de bibliothèque de stockage de fichiers
- Périphérique de bibliothèque de fichiers

### Périphérique de fichier autonome

Le périphérique de fichier autonome est le plus simple des systèmes de sauvegarde sur disque. Il se compose d'un simple logement dans lequel les données peuvent être sauvegardées. Une fois configurées, ses propriétés sont immuables. Le périphérique de fichier possède une capacité maximale de 2 To, si cette taille de fichier est prise en charge par le système d'exploitation sur lequel le périphérique fonctionne.

### Périphérique de bibliothèque de stockage de fichiers

Le périphérique de bibliothèque de stockage de fichiers est une version spéciale du périphérique de bibliothèque de stockage Data Protector. Le périphérique de bibliothèque de stockage peut être configuré pour sauvegarder des supports optiques ou des fichiers. Le périphérique de bibliothèque de stockage utilisé pour sauvegarder des fichiers est appelé périphérique de bibliothèque de stockage de fichiers. Le type

de supports sauvegardé par le périphérique de bibliothèque de stockage est spécifié pendant la configuration du périphérique.

Le périphérique de bibliothèque de stockage de fichiers se compose de plusieurs logements dans lesquels vous pouvez sauvegarder des données. La configuration est un processus en deux phases : on crée d'abord un périphérique de bibliothèque de stockage de fichiers, puis on configure un ou plusieurs lecteurs pour ce périphérique de bibliothèque de stockage. Une fois le périphérique configuré, il est possible de modifier ses propriétés. Chaque emplacement du périphérique de bibliothèque de stockage de fichiers a une capacité maximale de 2 To. La capacité maximale du périphérique est égale à :

Nombre de logements X 2 To

### Périphérique de bibliothèque de fichiers

Le périphérique de bibliothèque de fichiers est le plus perfectionné des systèmes de sauvegarde sur disque. Il dispose de multiples logements appelés **dépôts de fichier** dans lesquels vous pouvez sauvegarder des données. La configuration du périphérique de bibliothèque de fichiers s'effectue en une seule étape. Il est possible de modifier les propriétés du périphérique de bibliothèque de fichiers à tout moment. La capacité maximale de la bibliothèque est identique à la capacité maximale du système de fichiers sur lequel elle réside. Chaque dépôt de fichier possède une capacité maximale de 2 To. Les dépôts de fichier sont créés automatiquement selon les besoins.

Le périphérique de bibliothèque de fichiers utilise une gestion intelligente de l'espace disque. Il anticipe les problèmes potentiels liés à l'enregistrement des données. Un message d'avertissement est inscrit dans le journal des événements si l'espace disque disponible approche le minimum configuré requis pour que le périphérique fonctionne. Cela vous permet de libérer de l'espace disque à temps pour permettre au périphérique de continuer à enregistrer des données. Si l'ensemble de l'espace alloué au périphérique de bibliothèque de fichiers vient à être utilisé, un message d'avertissement apparaît à l'écran, avec des instructions permettant de résoudre le problème.

Le périphérique de bibliothèque de fichiers crée automatiquement de nouveaux dépôts de fichier si une sauvegarde particulière requiert plus d'espace que n'en contient un seul dépôt de fichier.

### Périphérique de sauvegarde sur disque recommandé

Hewlett-Packard recommande l'utilisation du périphérique de bibliothèque de fichiers en tant que périphérique favori de sauvegarde sur disque. Le périphérique de bibliothèque de fichiers est le plus flexible et le plus intelligent des périphériques de sauvegarde sur disque. Il est possible de le reconfigurer à tout moment pendant son utilisation et il est capable de gérer l'espace disque de manière plus perfectionnée



que les autres périphériques de sauvegarde sur disque. De plus, vous pourrez bénéficier de stratégies de sauvegarde avancées comme la sauvegarde synthétique.

Pour obtenir une description du fonctionnement du périphérique de bibliothèque, recherchez l'entrée suivante dans l'index de l'aide en ligne : "périphériques de bibliothèque de fichiers"

### Format de données

Le format de données des périphériques sur disque s'appuie sur le format de données pour bandes. Data Protector convertit au format de bande les données à sauvegarder avant de les écrire sur le périphérique sur disque.

Avec les bibliothèques de fichiers utilisées pour une **sauvegarde complète virtuelle**, il faut utiliser le format de supports de fichiers distribués. Sélectionnez ce format dans les propriétés du périphérique.

### Configuration

Il est possible de définir les propriétés de tous les périphériques sur disque pendant la configuration initiale des périphériques et après l'utilisation de ces derniers. Le degré de modification pouvant être apporté aux propriétés de chaque périphérique varie en fonction du périphérique.

### Sauvegarde sur un périphérique sur disque

Il est possible d'effectuer une sauvegarde sur un périphérique sur disque en créant une spécification de sauvegarde Data Protector normale.



---

# 10 Sauvegarde synthétique

## Dans ce chapitre

Le présent chapitre décrit le concept de la sauvegarde synthétique et les fonctions qu'offre en ce domaine Data Protector.

Il s'organise comme suit :

“Généralités” à la page 269

“Avantages de la sauvegarde sur disque” à la page 270

“Périphériques sur disque Data Protector” à la page 271

“Sauvegarde synthétique et restauration” à la page 278

## Généralités

La croissance du volume des données et la réduction de la fenêtre de sauvegarde rendent souvent problématique la réalisation d'une sauvegarde complète en termes de temps et d'espace de stockage. Par ailleurs, la possession d'un grand nombre de sauvegardes incrémentales peut poser problème, car chaque sauvegarde accroît le temps nécessaire pour effectuer une restauration.

La sauvegarde sur disque constitue une solution de plus en plus adoptée en raison d'un niveau élevé de performances et de capacité ainsi que de la baisse constante du coût des disques, et offre de nouvelles possibilités. Les exigences des entreprises consistent à réduire au minimum la fenêtre de sauvegarde et la charge sur les serveurs de production et le réseau, et à permettre une restauration rapide. La sauvegarde synthétique répond à ces exigences.

Il s'agit d'une solution de sauvegarde avancée qui produit une **sauvegarde complète synthétique**, équivalant à une sauvegarde complète classique en termes de données, sans créer de charge sur 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.

La réalisation d'une sauvegarde synthétique évite d'avoir à lancer régulièrement des sauvegardes complètes. Cette solution permet de réaliser des sauvegardes incrémentales aussitôt fusionnées avec la sauvegarde complète pour obtenir une nouvelle sauvegarde complète synthétique. Ce processus peut se répéter indéfiniment, sans besoin d'exécuter une autre sauvegarde complète.

En termes de vitesse de restauration, une telle sauvegarde est équivalente à une sauvegarde complète classique. La chaîne de restauration consiste en un seul élément, d'où une restauration aussi rapide et simple que possible.

## Avantages de la sauvegarde synthétique

La sauvegarde synthétique offre les avantages suivants :

- Elle évite d'avoir à réaliser des sauvegardes complètes. Après la sauvegarde complète initiale, seules des sauvegardes incrémentales sont effectuées, ce qui réduit beaucoup le temps nécessaire.
- La consolidation des objets sauvegardés s'effectue sur le serveur de périphériques, sans créer de charge sur les serveurs de production ou le réseau.
- Un type de sauvegarde synthétique, appelé sauvegarde complète virtuelle, offre encore plus d'efficacité. La sauvegarde complète virtuelle consiste à consolider les données à l'aide de pointeurs, ce qui évite une duplication inutile.
- Une restauration à partir d'une sauvegarde complète synthétique est aussi rapide qu'à partir d'une sauvegarde complète classique, car il n'est pas nécessaire de récupérer les données de sauvegardes incrémentales. Ceci évite la lecture de chaque sauvegarde incrémentale de la chaîne de restauration et également, en cas d'utilisation de périphériques à bande, le chargement et le déchargement de plusieurs supports ainsi que la recherche des versions d'objet.

## Fonctionnement de la sauvegarde synthétique Data Protector

La sauvegarde synthétique Data Protector permet de fusionner une sauvegarde complète et un nombre quelconque de sauvegardes incrémentales pour obtenir une nouvelle sauvegarde complète synthétique.

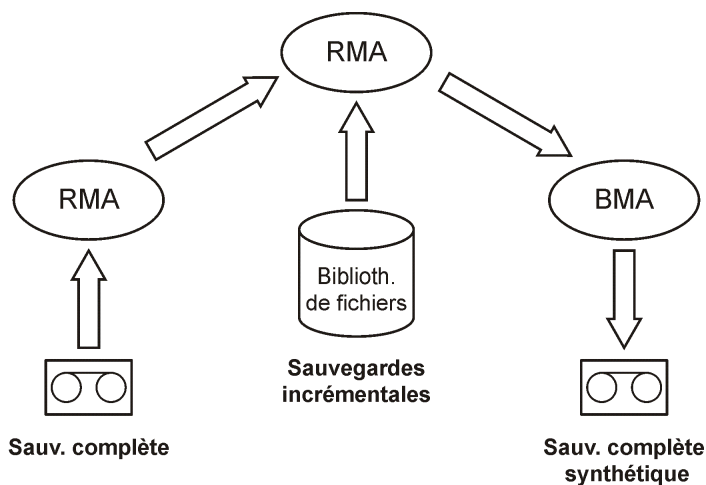
La sauvegarde synthétique exige l'utilisation de la sauvegarde incrémentale avancée. Il faut activer la sauvegarde incrémentale avancée avant de réaliser la sauvegarde complète et les sauvegardes incrémentales.

Il est possible de créer une sauvegarde complète synthétique à partir d'une sauvegarde complète écrite sur un périphérique à disque ou bande et de sauvegardes

incrémentales écrites sur un périphérique sur disque, une bibliothèque de fichiers Data Protector. La sauvegarde complète synthétique peut, quant à elle, être écrite sur un périphérique à disque ou bande.

Si toutes les sauvegardes, complètes et incrémentales, sont écrites dans la même bibliothèque de fichiers qui utilise le format de support de fichiers distribués, un type encore plus efficace de sauvegarde synthétique est disponible, appelé **sauvegarde complète virtuelle**. Cette technique utilise des pointeurs pour consolider les données au lieu de les copier. L'opération prend ainsi moins de temps et évite une duplication inutile des données.

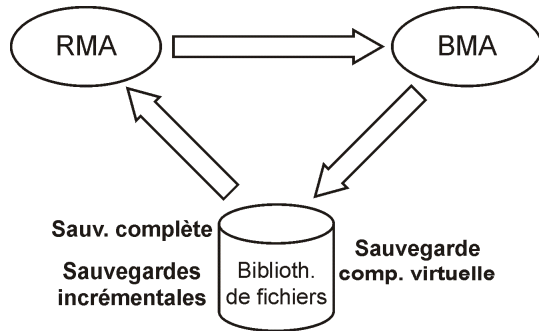
Les figures ci-dessous expliquent le concept de sauvegarde synthétique et de sauvegarde complète virtuelle. Elles indiquent comment une sauvegarde complète synthétique ou une sauvegarde complète virtuelle est créée à partir d'une sauvegarde complète et d'un certain nombre de sauvegardes incrémentales.



**Figure 67 Sauvegarde synthétique**

La [Figure 67](#) à la page 277 décrit le processus de création d'une sauvegarde complète synthétique. L'Agent de support de restauration (RMA) lit la sauvegarde complète sur le périphérique de sauvegarde (bande ou disque). Il transmet les données à un autre agent RMA, qui lit les sauvegardes incrémentales de la bibliothèque de fichiers et consolide les données. Les données consolidées sont ensuite transmises à l'Agent de support de sauvegarde (BMA), qui écrit la sauvegarde complète synthétique sur le périphérique de sauvegarde (bande ou disque).

En général, la sauvegarde complète synthétique est ensuite fusionnée avec des sauvegardes incrémentales ultérieures pour obtenir une nouvelle sauvegarde synthétique. Ce processus peut se répéter indéfiniment, après chaque sauvegarde incrémentale, ou à un intervalle souhaité.



**Figure 68 La sauvegarde complète virtuelle**

La Figure 68 à la page 278 décrit le processus de création d'une sauvegarde complète virtuelle. Pour ce type de sauvegarde, toutes les sauvegardes résident dans une seule bibliothèque de fichiers qui utilise le format de support de fichiers distribués. L'Agent de support de restauration (RMA) lit les informations sur la sauvegarde complète et les sauvegardes incrémentales, et génère les données pour la sauvegarde complète virtuelle. Les données générées sont transmises à l'Agent de support de sauvegarde (BMA), qui crée la sauvegarde complète virtuelle dans la bibliothèque de fichiers.

## Sauvegarde synthétique et utilisation d'espace de support

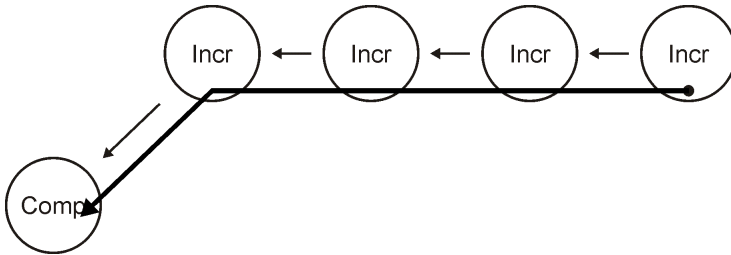
La réalisation fréquente de sauvegardes synthétiques et la conservation des sources impliquent en général une utilisation d'espace importante sur les supports de sauvegarde. Toutefois, la sauvegarde complète virtuelle permet de minimiser l'espace utilisé.

En cas de sauvegarde complète virtuelle, l'espace utilisé dépend en grande partie de la taille des fichiers sauvegardés. Si cette dernière est sensiblement supérieure à la taille de bloc utilisée, la sauvegarde complète virtuelle permet d'économiser l'espace au maximum par rapport à une sauvegarde synthétique normale. En revanche, si la taille des fichiers est inférieure à la taille de bloc, l'économie s'avère plutôt réduite.

## Sauvegarde synthétique et restauration

La restauration à partir d'une sauvegarde complète synthétique est équivalente à celle à partir d'une sauvegarde complète classique. Les figures ci-dessous présentent différentes situations, en supposant que vous devez restaurer des données dans leur dernier état possible. Tous les exemples supposent l'existence d'une sauvegarde

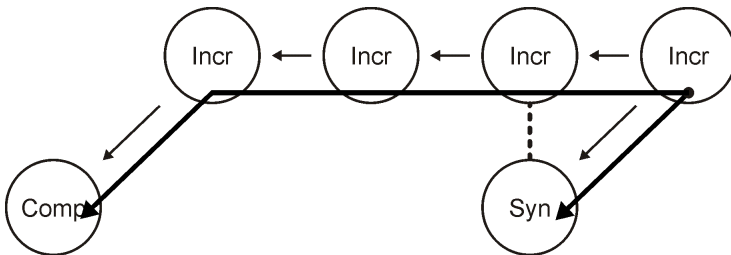
complète et de quatre sauvegardes incrémentales de l'objet sauvegarde. La différence réside dans l'utilisation de la sauvegarde synthétique.



**Figure 69 Sauvegardes complètes et incrémentales**

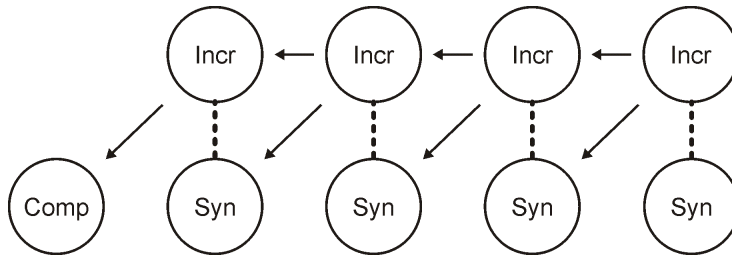
Dans la [Figure 69](#) à la page 279, des sauvegardes classiques ont été réalisées. Pour restaurer les données dans leur dernier état possible, vous avez besoin de la sauvegarde complète et des quatre sauvegardes incrémentales. La chaîne de restauration consiste en cinq éléments, qui résident souvent sur différents supports.

Une telle restauration peut prendre beaucoup de temps, car il faut lire chaque sauvegarde incrémentale. En cas d'utilisation de périphériques à bande, le chargement et le déchargement de plusieurs supports ainsi que la recherche des versions d'objet à restaurer prennent du temps.



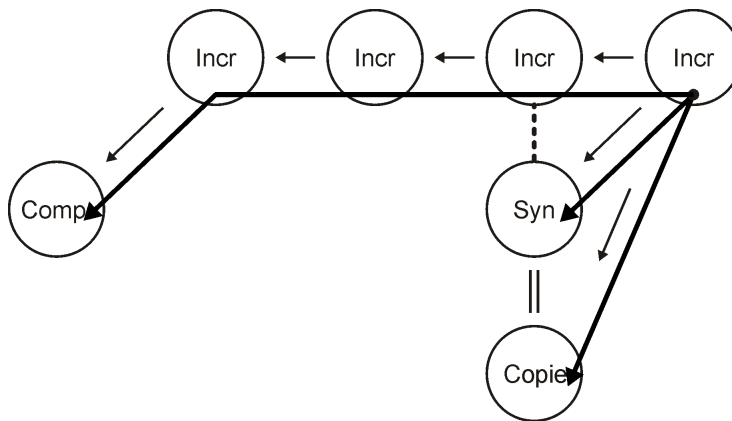
**Figure 70 Sauvegarde synthétique**

Dans la [Figure 70](#) à la page 279, une sauvegarde complète synthétique existe, qui sert à la restauration par défaut. La chaîne de restauration ne consiste qu'en deux éléments, à savoir la sauvegarde complète synthétique et la sauvegarde incrémentale ultérieure. La restauration est nettement plus simple et rapide que sans la sauvegarde complète synthétique. La figure illustre les deux chaînes de restauration possibles.



**Figure 71 Sauvegarde synthétique régulière**

La [Figure 71](#) à la page 280 montre une situation dans laquelle une sauvegarde synthétique a été réalisée après chaque sauvegarde incrémentale. Cette stratégie permet la restauration la plus simple et rapide dans le dernier état possible, ou à tout instant donné antérieur qui a fait l'objet d'une sauvegarde. La restauration n'exige qu'un seul élément, à savoir la sauvegarde complète synthétique de l'instant en question.



**Figure 72 Sauvegarde synthétique et copie d'objet**

Dans la [Figure 72](#) à la page 280, une sauvegarde synthétique a été réalisée, puis copiée. Ce processus offre plus de sécurité. La restauration dans le dernier état possible peut utiliser l'une des trois différentes chaînes de restauration indiquées. Par défaut, Data Protector sélectionne la chaîne de restauration optimale, qui inclut normalement la sauvegarde complète synthétique ou sa copie. En cas de support manquant, d'erreur de support ou similaire, une autre chaîne de restauration est utilisée.



## Influence des périodes de protection des données sur la restauration à partir d'une sauvegarde synthétique

La protection des données d'une sauvegarde complète classique et de toutes les sauvegardes incrémentales précédant une sauvegarde complète synthétique ne compromet pas la réussite de la restauration.

Par défaut, c'est la dernière sauvegarde complète synthétique dans la chaîne de sauvegarde qui est utilisée pour la restauration, même si les sauvegardes précédentes sont encore valables ou si leur protection a déjà expiré et les objets ont été supprimés de la base de données interne.

Pour plus de sécurité, choisissez une protection permanente afin que les données stockées sur les supports ne soient pas écrasées par accident.



---

# 11 Concepts Split Mirror

## Dans ce chapitre

Le présent chapitre décrit le concept de sauvegarde Split Mirror ainsi que les configurations prises en charge par HP.

Il s'organise comme suit :

“Généralités” à la page 283

“Configurations prises en charge” à la page 287

## Généralités

Aujourd'hui, les configurations de stockage modernes haute disponibilité (HA, pour High Availability) reflètent les nouvelles exigences en termes de sauvegarde. La configuration est l'une des nombreuses variations possibles de structures de miroir simple ou multiple.

L'approche générale consiste à utiliser une **réplique** (copie miroir) pour procéder à la sauvegarde, tandis que les **volumes sources** continuent à fonctionner pour l'application. Reportez-vous à la [Figure 73](#) à la page 284.

# Concept de sauvegarde SM

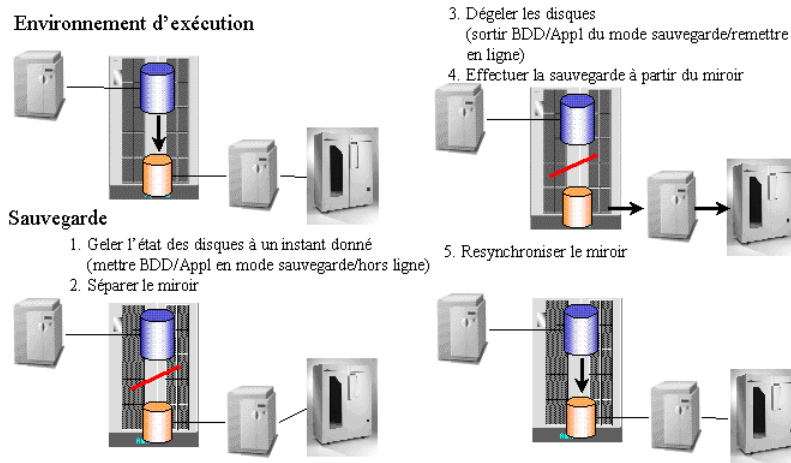


Figure 73 Concept de la sauvegarde Split Mirror

Les **volumes cibles** de la réplique sont généralement connectés à un client distinct, auquel sont également reliés des périphériques à bande pour les sauvegardes locales. Des technologies matérielles de mise en miroir telles que HP StorageWorks P9000 XP Disk Array Family ou EMC Symmetrix sont généralement utilisées pour créer une réplique telle que :

- HP Continuous Access P9000 XP ou
- HP Business Copy P9000 XP

L'application est disponible pratiquement en permanence, excepté pendant une courte période (qui peut aller de plusieurs secondes à quelques minutes). Au cours de cette période, le système assure la cohérence des données sur le disque et réalise la séparation effective des miroirs. Les données doivent être cohérentes pour que l'application puisse les utiliser après une restauration. En principe, la réplique miroir n'est pas créée au moment de la sauvegarde ; elle est déjà disponible et synchronisée à ce stade afin que l'application bénéficie d'une disponibilité élevée. La sauvegarde et la resynchronisation de la réplique n'affectent pas les performances de l'application, car ces opérations s'effectuent en parallèle, sur un autre équipement.

Le client d'application et celui de sauvegarde étant différents (dans la plupart des cas), toutes les données en cache (cache de la base de données, cache du système

de fichiers) du client doivent être transférées sur le disque avant que le miroir de la sauvegarde ne soit séparé. Pour cela, effectuez l'une des opérations suivantes :

- Placez les bases de données en mode sauvegarde.
- Mettez les bases de données hors ligne.
- Démontez un point de montage.

Une réplique ne sera cohérente que si vous effectuez ces opérations *préalablement* à la séparation. Cependant, si la base de données s'exécute sur un système de fichiers ou sur un rawdisk, il n'est pas nécessaire de démonter ce système de fichiers ou rawdisk, car la base de données s'assure que les données sont effectivement écrites sur le disque et non dans le cache du système de fichiers.

Dans le cas d'une sauvegarde de base de données en ligne, une réplique seule ne peut pas être restaurée. Les journaux d'archive du client d'application sont également requis. Vous pouvez démarrer une sauvegarde de journaux d'archive juste après la séparation, lorsque la base de données n'est plus en mode sauvegarde.

L'utilisation combinée d'une réplique et de la technologie HP Continuous Access P9000 XP pour réaliser la sauvegarde affecte la haute disponibilité du stockage pendant la durée de cette sauvegarde. Si vous disposez de miroirs supplémentaires, vous pouvez conserver la haute disponibilité de stockage tout en utilisant la même démarche de sauvegarde.

Le client de sauvegarde peut être le client central de plusieurs clients d'application exécutant différentes applications. Dans ce cas, le client de sauvegarde doit fonctionner sous le même système d'exploitation que le client d'application, afin d'accéder aux ressources mises en miroir de façon native.

Le client de sauvegarde doit pouvoir effectuer les sauvegardes dans un temps raisonnable. Bien qu'une sauvegarde puisse durer, en théorie, près de 24 heures, vous devez également prendre en compte le temps de restauration. Il est donc recommandé de prévoir un client de sauvegarde capable d'effectuer les sauvegardes en deux à quatre heures, et de réaliser les restaurations au moyen du client d'application.

Avec cette approche, la majeure partie du transfert des données s'effectue via le client de sauvegarde et son accès à la réplique. La connexion réseau entre le client de sauvegarde et le client d'application ne sert qu'à coordonner les processus impliqués dans la sauvegarde. De plus, des processus s'exécutent sur chaque client afin d'automatiser la séparation.

## Restauration instantanée

Data Protector assure une restauration instantanée reposant sur la technologie Split Mirror. La solution repose sur des solutions de sauvegarde avec temps d'indisponibilité

nul (ZDB) telles que l'intégration HP StorageWorks P9000 XP Disk Array Family, laquelle emploie principalement la technologie Split Mirror de la baie de disques.

Pendant une session de sauvegarde Split Mirror, une réplique est utilisée pour le transfert des données sur un support de sauvegarde (bande). Après la sauvegarde, vous pouvez supprimer la réplique et préparer deux disques pour la prochaine session de sauvegarde par resynchronisation, ou bien conserver la réplique en vue d'une restauration instantanée. Plusieurs répliques peuvent exister simultanément. Grâce à HP StorageWorks P9000 XP Disk Array Family, vous pouvez par exemple réaliser jusqu'à trois répliques Split Mirror, chacune d'elles pouvant être copiée deux fois si vous utilisez le traitement en cascade.

Pendant la restauration instantanée, les données présentes sur la réplique Split Mirror spécifiée (inchangée à des fins de restauration instantanée) sont synchronisées avec les volumes sources du client d'application et non restaurées depuis un support de sauvegarde.

Data Protector n'utilise que les trois premières répliques Split Mirror ; en effet, les copies miroir secondaires ne permettent pas d'assurer une resynchronisation rapide, laquelle est essentielle pour minimiser le temps de restauration. La restauration instantanée n'est possible qu'avec les configurations HP Business Copy P9000 XP (miroir local - hôte double et miroir local - hôte simple).

### Sauvegarde sur bande avec temps d'indisponibilité nul et ZDB sur disque + bande

Lors d'une session de sauvegarde sur bande ou sur disque + bande avec temps d'indisponibilité nul, une réplique des données d'application est écrite en flux continu sur un périphérique à bande connecté à un système de sauvegarde séparé, à l'aide de l'Agent de disque et de l'Agent général de support Data Protector, et ce avec une incidence minimale sur le système d'application. Une fois la sauvegarde terminée, la réplique est :

- supprimée - sauvegarde ZDB sur bande
- conservée en vue d'une restauration instantanée - sauvegarde ZDB sur disque + bande

### Sauvegarde ZDB sur disque

Pendant une session de sauvegarde sur disque avec temps d'indisponibilité nul, les données originales sont déplacées vers un support de sauvegarde (bande) à partir de la réplique. Les répliques (trois au maximum) peuvent servir à différentes fins, notamment au traitement de données hors ligne ou à la restauration instantanée ; cette dernière requiert l'utilisation de la configuration HP Business Copy P9000 XP. La restauration d'objets à partir d'une session de sauvegarde sur disque avec temps

d'indisponibilité nul n'est possible qu'avec la fonctionnalité de restauration instantanée.

### Rotation des jeux de répliques

Plusieurs répliques peuvent coexister. HP StorageWorks P9000 XP Disk Array Family permet de réaliser jusqu'à trois répliques Split Mirror, chacune d'elles pouvant être copiée deux fois dans le cas d'un traitement en cascade. Data Protector ne peut utiliser que les disques des trois premières répliques Split Mirror (**miroirs de premier niveau** ou **MU**) pour les opérations de sauvegarde et de restauration instantanée. Les six copies supplémentaires (miroirs en cascade) ne sont pas prises en charge. Lors de la configuration d'une spécification de sauvegarde avec temps d'indisponibilité nul pour un volume source (LDEV) avec des miroirs de premier niveau configurés ou lors de la restauration vers ce volume source, il est possible, en utilisant Data Protector, de définir un **jeu de répliques** à partir duquel cette intégration sélectionne une réplique pour la session en cours.

### Clients de sauvegarde et clusters

Le client de sauvegarde ne doit pas être utilisé comme serveur de basculement pour le client d'application. Il est recommandé d'installer les services d'application et de sauvegarde sur des clusters séparés.

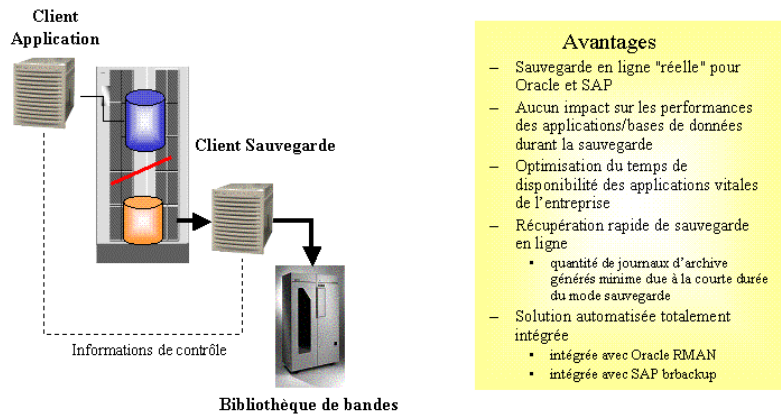
## Configurations prises en charge

### Miroir local - hôte double

Cette solution utilise une fonction de mise en miroir locale (HP Business Copy P9000 XP, par exemple). Les deux disques se trouvent dans la même baie de disques, ce qui signifie que l'infrastructure d'E/S du système RAID est partagée entre le client d'application (ou hôte) et le client de sauvegarde.

Le client d'application et le client de sauvegarde étant deux systèmes physiquement différents, ils peuvent utiliser leurs propres ressources (canaux d'E/S, processeurs, mémoire, etc.) pour réaliser leurs activités spécifiques (une sauvegarde, par exemple), sans incidence sur le fonctionnement de l'autre. Ainsi, les performances de la sauvegarde n'influent pas sur celles de la base de données.

## Miroir local – Hôte double sauvegarde avec temps d'indisponibilité nul et sans impact sur les performances



**Figure 74 Miroir local - hôte double (sauvegarde avec performances optimales et temps d'indisponibilité nul)**

L'intégration de sauvegarde Split Mirror Data Protector permet le traitement automatique de l'état du miroir, ainsi qu'une intégration étroite avec des applications telles que SAP R/3 et Oracle Server (afin d'assurer la cohérence des données et la prise en compte des sauvegardes par les applications/bases de données). Pour assurer une opération sécurisée et utiliser les outils d'application natifs pour la restauration, il faut que la sauvegarde soit prise en compte au préalable par l'application ou la base de données. L'impact d'une sauvegarde sur l'application est réduit au temps nécessaire pour effectuer une séparation du miroir et pour mettre la base de données dans un mode cohérent permettant la séparation, puis la faire quitter ce mode.

Cette configuration permet de réaliser en peu de temps une sauvegarde hors ligne à partir d'une base de données très volumineuse, ainsi qu'une sauvegarde en ligne générant très peu de journaux d'archive, la durée pendant laquelle la base de données reste en mode sauvegarde étant réduite au minimum.

Le fait de générer peu de journaux d'archive réduit l'espace nécessaire pour ce type de fichiers et accélère le processus de récupération de la base de données. Après la restauration d'une base de données en ligne, il est nécessaire d'effectuer une récupération afin que les données de la base redeviennent cohérentes. Tous les journaux d'archive ayant été créés au cours de la sauvegarde doivent être appliqués.



Dans le cas d'une sauvegarde Split Mirror, seuls les fichiers journaux d'archive créés au cours de la séparation sont appliqués.

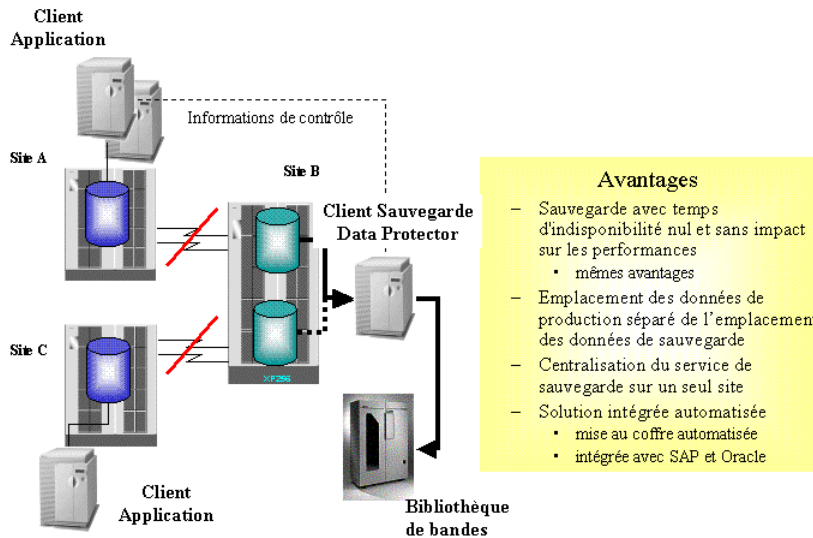
## Miroir local - hôte simple

Dans les cas où aucun serveur de sauvegarde dédié n'est disponible, les deux fonctions (application et sauvegarde) sont effectuées sur le même client (ou hôte). Les sauvegardes hors ligne des applications de messagerie, par exemple, peuvent réduire le temps d'indisponibilité de l'application de quelques heures à quelques minutes.

Dans ce type de configuration, seules les sauvegardes d'**image disque** (raw disk) et du **système de fichiers** sont prises en charge. Les sauvegardes de base de données et d'application, telles qu'Oracle Server et SAP R/3, ne peuvent pas être prises en charge car la base de données doit être montée sur le serveur de sauvegarde ; or, il n'est pas possible d'effectuer cette opération sur le serveur sur lequel la base de données est déjà montée.

## Miroir distant

La technologie de miroir distant, HP Continuous Access P9000 XP par exemple, améliore les configurations citées plus haut car les processus de sauvegarde et d'application utilisent différentes baies de disques à différents endroits.



**Figure 75 Split Mirror - miroir distant (sauvegarde distante indépendante du réseau local - données haute disponibilité)**

Le miroir distant transfère les données vers un site physiquement séparé. Celles-ci peuvent alors être sauvegardées sur des bandes disponibles en local. Cette opération permet de séparer les données de production des données de sauvegarde et par conséquent, d'éliminer le risque de dommages à ces deux types de données en même temps en cas d'incendie ou d'un autre sinistre.

Au cours d'une sauvegarde, la synchronisation des miroirs ne requiert aucune ressource réseau. Bien que les données ne soient pas transférées via le réseau, Data Protector a néanmoins besoin de la communication entre le Gestionnaire de cellule et ses clients.

Cette solution vous permet de centraliser un service de sauvegarde en mettant en miroir les données d'application provenant de plusieurs sites de production (A et C dans ce cas) dans un lieu unique ou une baie de disques centralisée. Ainsi, votre investissement dans un service de sauvegarde (serveur et bibliothèque de bandes) peut être consolidé et combiné avec la haute disponibilité d'une configuration à miroir distant.

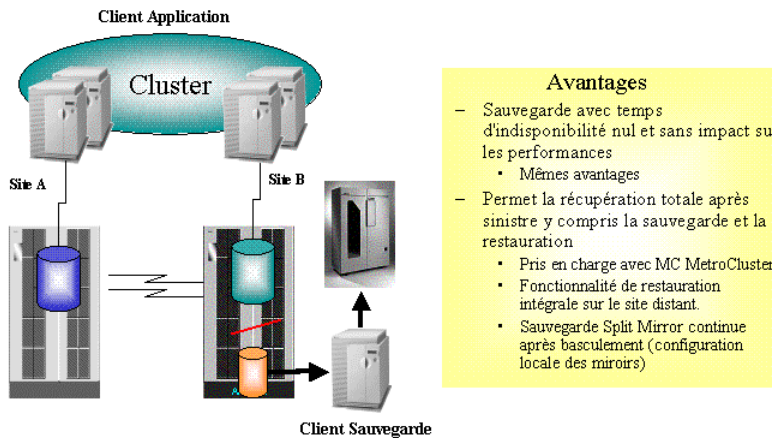
Le site distant ne peut pas être utilisé comme site de récupération après sinistre automatique pendant que la sauvegarde s'effectue, car le lien entre les deux sites est alors rompu (et les deux disques ne sont pas synchronisés). Ceci signifie qu'en

cas de défaillance du site A, le site B ne peut pas prendre le relais automatiquement (ce qu'il ferait normalement) pendant x heures (x correspondant au temps nécessaire pour que les données soient copiées sur la bande). Ce problème concerne également les mises en miroir locales. Toutefois, cela pose surtout des problèmes pour la solution distante, car le concept d'un site distant de récupération après sinistre distant faisant appel aux miroirs de matériel est largement répandu sur le marché.

## Combinaison de miroirs local et distant

Si le client a besoin de disposer en permanence d'un site de récupération disponible (fourni, par exemple, par un MetroCluster) et d'effectuer des sauvegardes avec un temps d'indisponibilité nul, il est possible de combiner le miroir distant avec le miroir local.

Cette solution présente tous les avantages du Split Mirror et permet d'effectuer une récupération complète vers le site distant. Dans cet exemple, le miroir distant est maintenu en permanence et le lien local n'est séparé que pour effectuer des sauvegardes. Le cluster peut donc basculer à tout moment sur le site distant (site B).



**Figure 76 Combinaison de miroirs local et distant (récupération après sinistre intégrée à la sauvegarde : service haute disponibilité - HP UX uniquement)**

Pour que la fonction de basculement soit indépendante de l'opération de sauvegarde, le client de sauvegarde doit être un autre client séparé et se trouver en dehors du cluster. Si une solution MetroCluster est mise en place, le client d'arbitrage de cluster peut être le client de sauvegarde.

## Autres configurations

Il existe de nombreuses autres configurations Split Mirror qui fournissent des avantages spécifiques ou répondent aux besoins de certains utilisateurs. Toutefois, chacune est associée à un modèle de comportement spécifique représentant des exigences particulières auxquelles les fonctions de contrôle doivent obéir afin de garantir la sauvegarde et la récupération. Il est donc important de vérifier quelles configurations sont prises en charge et de les spécifier.

Toutes les configurations décrites précédemment sont prises en charge par HP. Pour obtenir la liste actualisée des configurations prises en charge, consultez les dernières matrices de support à l'adresse <http://www.hp.com/support/manuals>.

Si une configuration dans laquelle vous souhaitez sauvegarder des données n'est pas répertoriée dans la liste, cela ne signifie pas que l'opération ne peut pas être

prise en charge. Contactez votre représentant HP local ou votre consultant HP pour connaître les autres configurations prises en charge.



---

# 12 Concepts de snapshot

## Dans ce chapitre

Le présent chapitre décrit le concept de sauvegarde de snapshot, ainsi que les configurations prises en charge par HP.

Il s'organise comme suit :

“Généralités” à la page 295F

“Configurations prises en charge” à la page 301

## Généralités

Pour répondre à la demande croissante en configurations de stockage haute disponibilité, de nouvelles technologies de sauvegarde avec temps d'indisponibilité nul ont été mises au point . D'autre part, les progrès en matière de technologie de virtualisation de stockage procurent aujourd'hui une alternative à la technologie Split Mirror conventionnelle.

La solution de sauvegarde à temps d'indisponibilité nul Data Protector associe différentes technologies de baies de disques aux derniers développements en matière de technologie de "snapshot" (image figée) pour créer des snapshots de données d'applications ou de bases de données enregistrées sur une baie de disques. Ces snapshots peuvent ensuite être conservés sur une baie de disques sous forme de copies ponctuelles des données d'origine à des fins de **restauration instantanée**, ou peuvent être utilisées pour créer des sauvegardes sur bande avec temps d'indisponibilité nul sur un système de sauvegarde. Les processus impliqués ont peu d'impact sur le serveur d'applications, offrant ainsi une solution réelle en termes de sauvegarde avec temps d'indisponibilité nul.

## Virtualisation du stockage

Le terme "virtualisation du stockage" fait référence à la technologie qui permet de séparer la représentation logique du stockage des composants de stockage physiques

réels. Elle implique la création de volumes logiques en dehors d'un pool de disques physiques résidant sur une baie de disques. Un volume logique est limité au cadre du pool mais peut s'étendre sur un nombre quelconque de disques physiques au niveau de la baie de disques. Un ou plusieurs systèmes hôtes peuvent utiliser les volumes logiques. Il est impossible de gérer précisément l'allocation de volumes logiques sur des disques physiques ; différentes options de protection permettent toutefois de définir une orientation.

## RAID

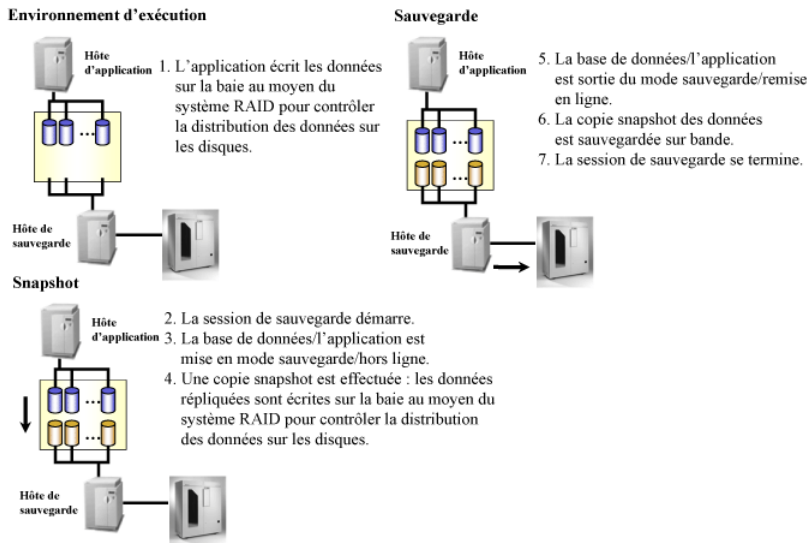
La technologie RAID (Redundant Array of Independent Disks, ou baie de disques redondants indépendants) permet de définir le mode de distribution des données sur les disques physiques au niveau d'une baie de disques. Il existe différents niveaux RAID, correspondant à différents niveaux de redondance et de sécurité de données, de taux de transfert et de temps d'accès. Par exemple, le niveau RAID0 n'implique aucune duplication des données, RAID1 implique la duplication de toutes les données et RAID5 implique la protection des données par parité.

Les fonctions de snapshot Data Protector intégrées ont été conçues pour être utilisées avec des baies de disques prenant en charge les technologies de snapshot, telles que HP StorageWorks P6000 EVA Disk Array Family ou HP StorageWorks P4000 SAN Solutions.

## Concepts de snapshot

Dans une configuration de base standard utilisant la technologie de snapshot, une baie de disques individuelle peut être connectée à des systèmes d'application et de sauvegarde séparés. La baie de disques peut être utilisée comme périphérique de stockage par le système d'application et le système de sauvegarde, et les volumes logiques peuvent être montés sur l'un ou l'autre. Lorsque ce schéma est appliqué, le système d'application utilise les volumes logiques de la baie de disques pour le stockage de ses données en période de fonctionnement normal. Les volumes logiques sur lesquels sont stockées les données du système d'application pour les besoins des fonctions de snapshot Data Protector intégrées sont également appelés **volumes sources**. Lorsqu'une sauvegarde de snapshot est réalisée, les données d'application résidant au niveau des volumes sources sont dupliquées et écrites sur d'autres volumes logiques de la même baie de disques, également appelés **volumes cibles**. Les données ainsi dupliquées sont également appelées données snapshot. Elles correspondent à des copies ponctuelles instantanées d'un système de fichiers ou d'un volume donné. L'ensemble des volumes cibles ainsi créés est également appelé **réplique**. Une fois la réplique des données snapshot créée, il est possible d'apporter des modifications aux données d'origine sans perturber le déroulement de l'opération de sauvegarde.





**Figure 77 Sauvegarde de snapshot**

Le client de sauvegarde est configuré comme client Data Protector auquel des périphériques à bande sont connectés en vue de réaliser des sauvegardes en local.

Lorsqu'une session de sauvegarde commence, le client d'application passe en mode sauvegarde tandis que le système prépare le client de sauvegarde en vue de la procédure de sauvegarde ; un snapshot des données d'application est créé.

Lorsque le client de sauvegarde est prêt et que la réplique des données snapshot est créée, l'application revient en mode de fonctionnement normal.

Le niveau de disponibilité de l'application reste pratiquement inchangé pendant que le client d'application est en mode sauvegarde (dans certains cas, l'application peut être arrêtée pendant un bref laps de temps).

Si l'on a spécifié une sauvegarde sur bande avec temps d'indisponibilité nul, les données snapshot sont ensuite écrites en flux continu sur des supports à bande au niveau du client de sauvegarde. Cette opération ne perturbe pas le fonctionnement du client d'application.

Les clients d'application et de sauvegarde étant généralement distincts, il est impératif de transférer toutes les informations mises en cache (caches de la base de données et du système de fichiers) du client d'application vers la baie de disques avant la création du snapshot. Pour cela, effectuez l'une des opérations suivantes :

- Placez les bases de données en mode sauvegarde.
- Mettez les bases de données hors ligne.
- Démontez un point de montage.

Dans le cas d'une sauvegarde de base de données en ligne, les données snapshot ne permettent pas à elles seules de procéder à la restauration. Les journaux d'archive du client d'application sont également requis. Une procédure de sauvegarde standard Data Protector peut être utilisée pour effectuer une sauvegarde de journaux d'archive immédiatement après la création des snapshots, lorsque que la base de données n'est plus en mode sauvegarde.

Les données de snapshot correspondant aux données d'application peuvent être créées au moyen de technologies de baies de disques virtuelles, telles que HP StorageWorks P6000 EVA Disk Array Family ou HP StorageWorks P4000 SAN Solutions.

## Types de sauvegardes de snapshot

Les types de sauvegardes de snapshot suivants sont disponibles dans le cadre des fonctions de snapshot Data Protector intégrées :

- sauvegarde ZDB sur bande
- sauvegarde ZDB sur disque
- sauvegarde ZDB sur disque + bande

### Sauvegarde sur bande avec temps d'indisponibilité nul et ZDB sur disque + bande

Lors d'une session de sauvegarde sur bande ou sur disque + bande avec temps d'indisponibilité nul, un snapshot des données d'application réalisé à un instant donné est écrit en flux continu sur un périphérique à bande connecté à un système de sauvegarde séparé, à l'aide de l'Agent de disque et de l'Agent général de support Data Protector, et ce avec une incidence minimale sur le système d'application. Une fois la sauvegarde terminée, les données snapshot sont :

- supprimée - sauvegarde ZDB sur bande
- conservée en vue d'une restauration instantanée - sauvegarde ZDB sur disque + bande

### Sauvegarde ZDB sur disque

La technologie employée lors d'une session de sauvegarde sur disque avec temps d'indisponibilité nul est identique à celle utilisée lors d'une sauvegarde sur bande ou ZDB sur disque + bande ; toutefois, les données snapshot ne sont pas écrites en flux continu sur un support de sauvegarde (périphérique à bande) à partir de la

copie snapshot mais sont conservées sur une baie de disques. Elles peuvent être utilisées pour la restauration instantanée. La session se termine dès que les données snapshot sont créées.

## Restauration instantanée

Pendant les sessions de sauvegarde de snapshot, plusieurs copies snapshot des données peuvent être produites et conservées sur une baie de disques, chaque copie étant effectuée à un instant donné dans sa propre réplique. Les copies snapshot conservées peuvent ensuite être utilisées pour la restauration instantanée, le traitement de données hors ligne ou à d'autres fins. Seules les copies ponctuelles générées lors de sessions de sauvegarde sur disque ou sur disque + bande avec temps d'indisponibilité nul peuvent être restaurées au moyen de la fonctionnalité de restauration instantanée.

En cas de restauration instantanée, la copie ponctuelle d'une réplique sélectionnée est restaurée sur une baie de disques dans l'état dans lequel elle se trouvait au moment où les données snapshot ont été générées. Aucun transfert de données à partir d'un support de bande n'étant requis dans le cadre de cette procédure, la durée de restauration globale est considérablement réduite.

Les journaux d'archive d'application ne sont pas compris dans une sauvegarde de snapshot ; par conséquent, il est nécessaire de les récupérer à partir de supports à bande pour les restaurer et les utiliser.

## Jeu de répliques et rotation d'un jeu de répliques

Le nombre maximal de répliques pouvant être conservées simultanément sur une baie de disques dépend de la baie de disques utilisée. Les répliques conservées sur une baie de disques dans le cadre d'une même spécification de sauvegarde constituent le **jeu de répliques** de cette spécification de sauvegarde. Le jeu de répliques dépend du nombre maximal de répliques pouvant être conservées sur une baie de disques dans le cadre d'une spécification de sauvegarde donnée. Lorsque cette limite maximale est atteinte lors d'une session de sauvegarde de snapshot, les données de snapshot de la réplique la plus ancienne du jeu de répliques sont écrasées. Tant que la limite n'est pas atteinte, le système crée une nouvelle réplique. Ces deux opérations s'inscrivent dans le cadre de la procédure de **rotation du jeu de répliques**.

## Types de snapshots

Suivant la baie de disques utilisée, différents types de snapshots peuvent être employés lors d'une session de sauvegarde de snapshot Data Protector. Les types de snapshots suivants sont utilisés dans le cadre des fonctions de snapshot Data Protector intégrées :

- Snapshots de type copie par écriture (copy-on-write) avec préallocation d'espace disque
- Snapshots de type copie par écriture (copy-on-write) sans préallocation d'espace disque
- Snapclones

### Snapshots avec préallocation d'espace disque

La création de snapshots de type copie par écriture (copy-on-write) avec préallocation d'espace disque requiert la même quantité d'espace disque que celle allouée au volume source. Les données ne sont écrites sur cet espace réservé qu'en cas de besoin. Les modifications apportées aux données du volume source sont répercutées sur les données snapshot du volume cible.

Dans le cadre du système de snapshot, seules les modifications apportées aux données d'origine (en constante évolution) par rapport à un état donné sont mises en cache ; c'est la raison pour laquelle les snapshots de type copie par écriture (copy-on-write) avec préallocation d'espace disque sont tributaires de leurs volumes sources : si les données des volumes sources sont perdues, les snapshots associés sont inutilisables.

### Snapshots sans préallocation d'espace disque

Les snapshots de type copie par écriture (copy-on-write) sans préallocation d'espace disque correspondent également à une copie ponctuelle des données d'origine mais ne requièrent pas de préallocation d'espace disque. L'espace disque est alloué à la demande de façon dynamique. Lorsque des modifications sont apportées aux données du volume source, le système utilise l'espace disponible sur une baie de disques pour la création du snapshot. Les snapshots de type copie par écriture (copy-on-write) sans préallocation d'espace disque ne sont utiles qu'à court terme. Notez que la taille de ces snapshots augmente de façon dynamique : si l'on ne supprime pas régulièrement ces snapshots, les capacités de stockage risquent d'être saturées.

Le principal avantage des snapshots de type copie par écriture (copy-on-write) sans préallocation d'espace disque, par rapport à ceux avec préallocation d'espace disque, tient au fait qu'ils permettent de réduire les coûts de façon significative. Si les snapshots sont supprimés régulièrement, cette technologie requiert beaucoup moins d'espace de stockage pour la duplication que la technologie de snapshot standard.

Dans le cadre du système de snapshot, seules les modifications apportées aux données d'origine (en constante évolution) par rapport à un état donné sont mises en cache ; c'est la raison pour laquelle les snapshots de type copie par écriture (copy-on-write) sans préallocation d'espace disque sont tributaires de leurs volumes sources : si les données des volumes sources sont perdues, les snapshots associés sont inutilisables.

## Snapclones

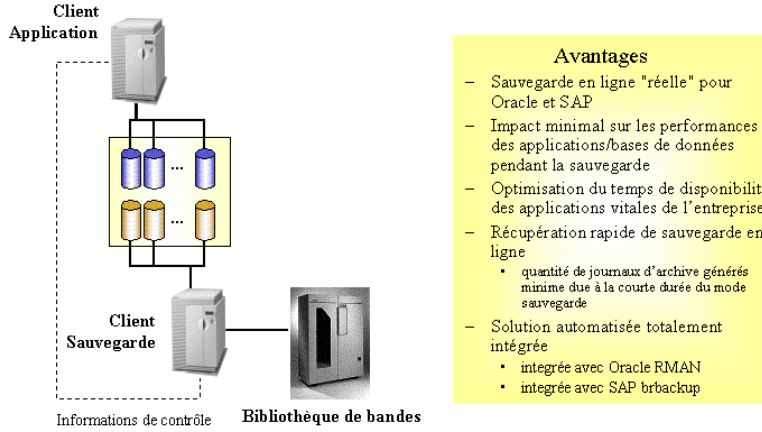
La création des snapclones commence par une procédure semblable à celle utilisée pour créer des snapshots de type copie par écriture (copy-on-write) sans préallocation d'espace disque. Elle est suivie du processus de clonage. Pendant ce processus, toutes les données du volume source sont copiées dans le volume cible. Un snapclone permet d'accéder immédiatement aux données répliquées pendant que le processus de clonage s'exécute en tâche de fond en exploitant les périodes d'inactivité de la baie de disques. Une fois le processus de clonage achevé, le snapclone est une copie de données complète reproduisant le volume source à un état donné ; si les données stockées sur le volume source sont perdues, vous pouvez toujours rétablir le snapclone.

# Configurations prises en charge

## Configuration de base : baie de disques simple - hôte double

Les deux hôtes sont connectés à la même baie de disque, de sorte que l'infrastructure d'E/S du système RAID soit partagée entre le client d'application et le client de sauvegarde.

Le client d'application et le client de sauvegarde étant deux systèmes physiquement différents, ils peuvent utiliser leurs propres ressources (canaux d'E/S, processeurs, mémoire, etc.) pour réaliser leurs activités spécifiques (une sauvegarde, par exemple), sans incidence sur le fonctionnement de l'autre. Ainsi, l'impact de la sauvegarde sur les performances de la base de données est minime.



**Figure 78 Baie de disques simple - hôte double (sauvegarde avec performance optimale et temps d'indisponibilité nul)**

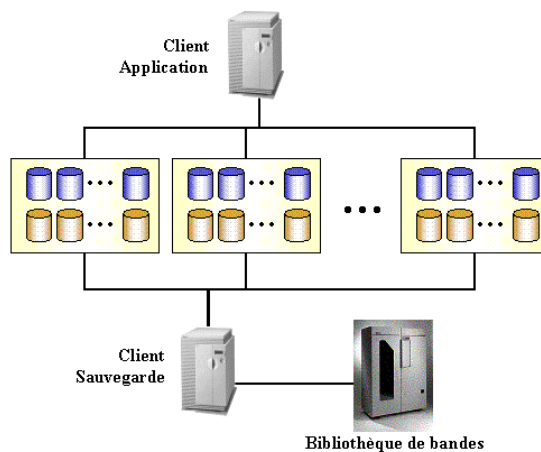
Les fonctions de snapshot Data Protector intégrées permettent le traitement automatique de l'état des baies de disques ainsi qu'une intégration parfaite avec des applications telles que SAP R/3, Oracle Server, Microsoft SQL Server ou Microsoft Exchange Server (afin d'assurer la cohérence des données et la prise en compte des sauvegardes par les bases de données/applications). Pour assurer une opération sécurisée et utiliser les outils d'application natifs pour la restauration, il faut que la sauvegarde soit prise en compte au préalable par l'application ou la base de données. En cas de sauvegarde, le fonctionnement de l'application n'est affecté que le temps nécessaire pour effectuer les opérations suivantes :

1. Réorganisation de la base de données afin d'en assurer la cohérence en vue de la génération d'un snapshot.
2. Réalisation d'un snapshot des données d'application.
3. Rétablissement du mode de fonctionnement normal de la base de données.

Cette configuration permet de réaliser en peu de temps une sauvegarde hors ligne à partir d'une base de données très volumineuse, ainsi qu'une sauvegarde en ligne générant très peu de journaux d'archive, la durée pendant laquelle la base de données reste en mode sauvegarde étant réduite au minimum.

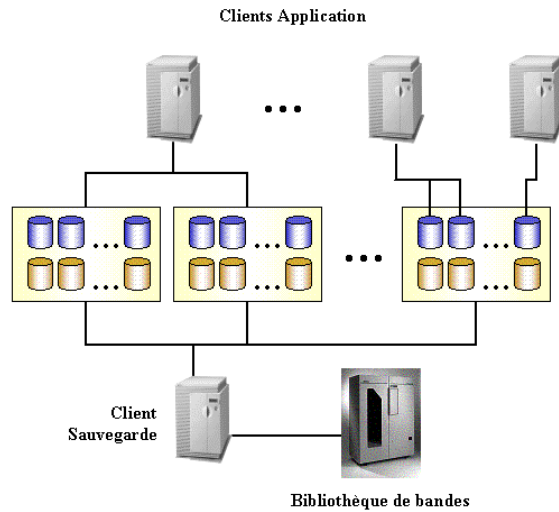
Le fait de générer peu de journaux d'archive réduit l'espace nécessaire pour ce type de fichiers et accélère la procédure de récupération de la base de données. Après la restauration d'une base de données en ligne, il est nécessaire d'effectuer une récupération afin que les données de la base redeviennent cohérentes. Tous les journaux d'archive ayant été créés au cours de la sauvegarde doivent être appliqués. Au cours d'une sauvegarde de snapshot, seuls les journaux d'archive créés au cours du snapshot sont utilisés.

## Autres configurations prises en charge



**Figure 79 Baies de disques multiples - hôte double**

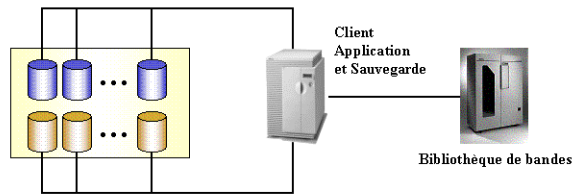
Avec cette solution, les deux hôtes sont connectés à plusieurs baies de disques. L'infrastructure d'E/S des systèmes RAID est partagée entre le client d'application et le client de sauvegarde.



**Figure 80 Hôtes d'application multiples - hôte de sauvegarde simple**

Avec cette solution, plusieurs hôtes d'application peuvent être connectés à une ou plusieurs baies de disques, elles-mêmes connectées à un hôte de sauvegarde simple dédié. L'infrastructure d'E/S des systèmes RAID est partagée entre les clients d'application et le client de sauvegarde.





**Figure 81 Baie(s) de disques - hôte simple**

Dans les cas où aucun serveur de sauvegarde dédié n'est disponible, les deux fonctions (application et sauvegarde) peuvent être effectuées sur le même client (ou hôte). Les sauvegardes hors ligne des applications de messagerie, par exemple, peuvent réduire le temps d'indisponibilité de l'application de quelques heures à quelques minutes.

### Clients de sauvegarde et clusters

Le client de sauvegarde ne doit pas être utilisé comme serveur de basculement pour le client d'application. Il est recommandé d'installer les services d'application et de sauvegarde sur des clusters séparés.

### Autres configurations

Il existe d'autres configurations de baie de disques qui fournissent des avantages spécifiques ou répondent à des besoins particuliers. Toutefois, chacune est associée à un modèle de comportement spécifique représentant des exigences particulières auxquelles les fonctions de contrôle doivent obéir afin de garantir la sauvegarde et la récupération. Il est donc important de vérifier quelles configurations sont prises en charge et de les spécifier.

Seules les configurations indiquées sont prises en charge par HP. Pour obtenir la liste actualisée des configurations prises en charge, consultez les dernières matrices de support à l'adresse <http://www.hp.com/support/manuals>.

Si une configuration dans laquelle vous souhaitez sauvegarder des données n'est pas répertoriée dans la liste, cela ne signifie pas que l'opération ne peut pas être prise en charge. Contactez votre représentant HP local ou votre consultant HP pour connaître les autres configurations prises en charge.

---

# 13 Microsoft Volume Shadow Copy Service

## Dans ce chapitre

Ce chapitre présente le concept de Microsoft Volume Shadow Copy Service (VSS) et son rôle dans le processus de sauvegarde et de restauration. Il indique également le processus de sauvegarde et de restauration que permet cette fonction.

Le chapitre est organisé de la façon suivante :

“Généralités” à la page 307

“Intégration de Data Protector à Volume Shadow Copy Service” à la page 312

“Sauvegarde et restauration de système de fichiers VSS” à la page 313

Pour obtenir des informations détaillées sur l'intégration, reportez-vous au *Guide d'intégration HP Data Protector*. Pour obtenir des informations détaillées sur la sauvegarde et la restauration de système de fichiers, reportez-vous à l'aide en ligne de Data Protector.

## Généralités

Le processus de sauvegarde traditionnel est basé sur la communication directe entre l'application de sauvegarde (l'application qui lance et exécute la sauvegarde) et l'application à sauvegarder. Cette méthode de sauvegarde nécessite que l'application de sauvegarde dispose d'une interface distincte pour chaque application sauvegardée.

Le nombre d'applications présentes sur le marché ne cesse de croître. La nécessité de gérer des fonctions spécifiques à une application peut entraîner des difficultés dans les activités de sauvegarde, de restauration et de stockage. Pour résoudre ce problème, une solution efficace consiste à mettre en place un coordinateur entre les différents acteurs du processus de sauvegarde et de restauration.

**Volume Shadow Copy Service (VSS)** est un service logiciel créé par Microsoft pour les systèmes d'exploitation Windows. Ce service collabore avec l'application de sauvegarde, les applications à sauvegarder, les fournisseurs de copies miroir et le noyau du système d'exploitation pour mettre en œuvre la gestion des copies miroir des volumes et des jeux de copies miroir.

Le logiciel Volume Shadow Copy Service vise à fournir une interface de communication unifiée, capable de coordonner la sauvegarde et la restauration de toute application, quelles que soient ses fonctionnalités spécifiques. Ainsi, l'application de sauvegarde n'a plus à gérer individuellement chaque application à sauvegarder. Toutefois, cette procédure n'est applicable à une application de sauvegarde que si celle-ci est conforme à la spécification VSS.

### Qu'est-ce qu'une copie miroir ?

Le terme **copie miroir** désigne un volume représentant une copie du volume d'origine à un moment donné. La technologie de copie miroir du volume fournit une copie 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.

La copie miroir n'est rien d'autre que la sauvegarde d'une image instantanée, laquelle permet aux applications et aux utilisateurs de continuer à saisir des données dans les volumes, même pendant un processus de sauvegarde, tandis que la sauvegarde récupère les données à partir d'une copie miroir du volume d'origine.

Un jeu de copies miroir est un ensemble de copies miroir créées au même instant.

### Qu'est-ce qu'un module d'écriture ?

Le terme **module d'écriture** désigne tout processus apportant une modification aux données du volume d'origine. Les modules d'écriture sont habituellement des applications (telles que MSDE Writer pour MS SQL Server) ou des services système (par exemple, System Writer et Registry Writer) qui copient des informations permanentes sur un volume. Ils participent au processus de synchronisation des copies miroir en assurant la cohérence des données.

### Qu'est-ce qu'un fournisseur de copie miroir ?

Le terme **fournisseur de copie miroir** désigne une entité qui exécute le travail nécessaire à la création et à la représentation des copies miroir des volumes. Les fournisseurs de copies miroir possèdent les données des copies miroir et exposent les copies miroir. Le fournisseur de copie miroir peut être de type logiciel (par exemple un

fournisseur système, MS Software Shadow Copy Provider) ou matériel (disques locaux, baies de disques).

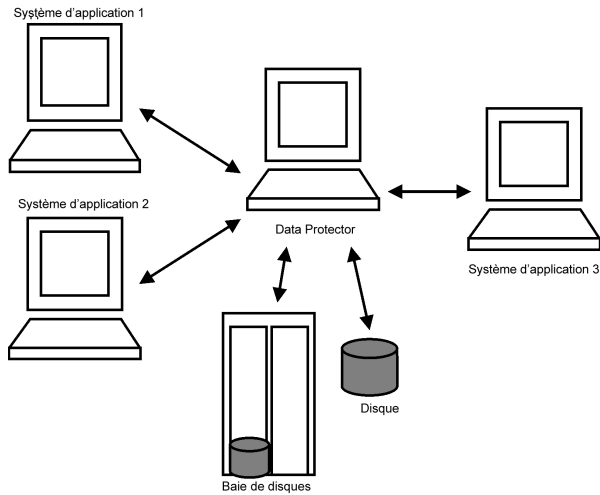
Une baie de disques est un exemple type de fournisseur matériel : elle possède son propre mécanisme matériel qui indique l'état d'un disque à un instant T. Un fournisseur matériel fonctionne sur des disques physiques et utilise un mécanisme logiciel pour fournir des indications sur l'état d'un disque à un instant T. Le fournisseur système, MS Software Shadow Copy Provider, est un mécanisme logiciel intégré aux systèmes d'exploitation Windows depuis Windows Server 2003.

Le mécanisme VSS garantit que tous les fournisseurs matériels seront proposés pour la création d'une copie miroir avant tous les fournisseurs logiciels. Si aucun d'eux n'est en mesure de créer une copie miroir, VSS fait appel pour cela à MS Software Shadow Copy Provider, lequel est toujours disponible.

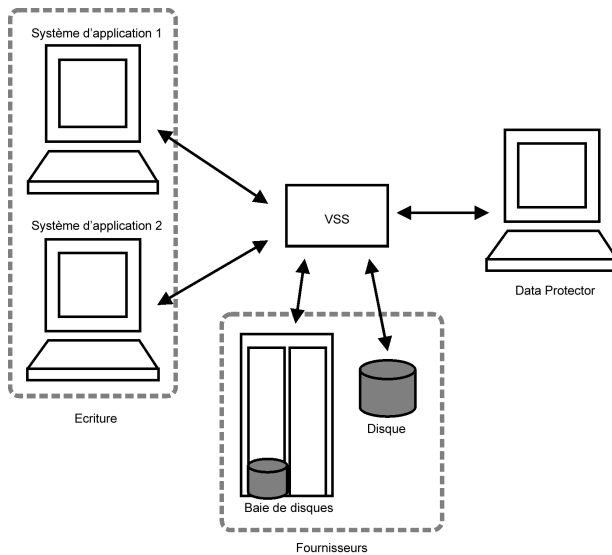
### Data Protector et VSS

Volume Shadow Copy Service permet de coordonner l'application de sauvegarde, les modules d'écriture et les fournisseurs de copies miroir pendant le processus de sauvegarde et de restauration.

La [Figure 82](#) à la page 310 et la [Figure 83](#) à la page 310 présentent les différences qui existent entre le modèle de sauvegarde traditionnel et le modèle doté du coordinateur VSS.



**Figure 82 Acteurs du modèle de sauvegarde traditionnel**



**Figure 83 Acteurs du modèle de sauvegarde VSS**

Dans le modèle traditionnel, l'application de sauvegarde devait communiquer individuellement avec chaque application qu'elle sauvegardait. Dans le modèle VSS, l'application de sauvegarde ne communique qu'avec le service VSS, lequel coordonne l'ensemble du processus de sauvegarde.

## Avantages du VSS

Volume Shadow Copy Service présente les avantages suivants :

- Une interface de sauvegarde unifiée pour tous les modules d'écriture
- Une interface de sauvegarde unifiée pour tous les fournisseurs de copies miroir
- Les modules d'écriture assurent l'intégrité des données au niveau de l'application. Aucune intervention de l'application de sauvegarde n'est nécessaire.

Data Protector prend en charge Microsoft Volume Shadow Copy Service à deux niveaux :

- Dans le cadre de l'intégration à Microsoft Volume Shadow Copy Service, Data Protector permet une sauvegarde et une restauration par copie miroir des modules d'écriture VSS, avec temps d'indisponibilité nul et restauration instantanée.
- Dans le cadre de la fonctionnalité Agent de disque, Data Protector permet une sauvegarde de système de fichiers VSS.

L'intégration Data Protector VSS ne prend en charge une sauvegarde en copie miroir cohérente que pour les modules d'écriture VSS. Dans ce cas, la cohérence est assurée par le module d'écriture. Lorsque les applications ne sont pas de type VSS, une copie miroir est créée. La cohérence des données de la copie miroir n'est pas garantie au niveau de l'application, mais elle est supérieure à celle que fournirait la sauvegarde d'un système de fichiers de type non-VSS.

Le tableau ci-dessous indique les différences entre la sauvegarde d'intégration Data Protector VSS, la sauvegarde d'un système de fichiers VSS et la sauvegarde d'un système de fichiers non-VSS :

**Tableau 14 Avantages de l'utilisation de VSS**

	<b>Sauvegarde de l'intégration Data Protector VSS</b>	<b>Sauvegarde de système de fichiers VSS</b>	<b>Sauvegarde de système de fichiers non-VSS</b>
Fichiers ouverts	Fichiers non ouverts	Fichiers non ouverts	Si les fichiers sont ouverts, la sauvegarde risque d'échouer.
Fichiers verrouillés	Fichiers non verrouillés	Fichiers non verrouillés	Si les fichiers sont verrouillés, la sauvegarde les ignore.

	<b>Sauvegarde de l'intégration Data Protector VSS</b>	<b>Sauvegarde de système de fichiers VSS</b>	<b>Sauvegarde de système de fichiers non-VSS</b>
Intégrité des données	Fournie par le module d'écriture.	Cohérence des données en cas de panne (par exemple en cas de panne d'alimentation).	Aucune (inhérent)

## Intégration de Data Protector à Volume Shadow Copy Service

L'intégration de Data Protector à Microsoft Volume Shadow Copy Service offre une prise en charge complète pour les modules d'écriture VSS, notamment la détection automatique des modules d'écriture VSS ainsi que la sauvegarde et la restauration. Pour obtenir des informations détaillées sur l'intégration, reportez-vous au *Guide d'intégration HP Data Protector*.

### Sauvegarde VSS

En cas de sauvegarde de modules d'écriture VSS, la cohérence des données est assurée au niveau du module et ne dépend pas de l'application de sauvegarde. Data Protector respecte les critères fournis par les modules d'écriture lors de la sélection des données à sauvegarder.

Au cours de la sauvegarde de modules d'écriture VSS, Data Protector ne communique pas avec les modules d'écriture individuellement, mais via l'interface VSS. Il utilise l'agent d'intégration VSS pour la liaison à Volume Shadow Copy Service, lequel coordonne le processus de sauvegarde. VSS fournit à Data Protector les métadonnées liées au module d'écriture qui sont nécessaires à la cohérence de la sauvegarde et de la restauration. Data Protector examine ces données, identifie les volumes à sauvegarder et demande ensuite à VSS de créer une copie miroir des volumes spécifiés.





## REMARQUE :

Un **document de métadonnées de module d'écriture** (WMD) regroupe les métadonnées fournies par chaque module d'écriture. Les modules d'écriture sont identifiés par les métadonnées qu'ils contiennent et indiquent à l'application de sauvegarde les données à sauvegarder et la procédure à suivre pour les restaurer. Data Protector respecte les critères fournis par le module d'écriture lors de la sélection des volumes à sauvegarder et de la méthode de restauration.

Volume Shadow Copy Service synchronise les modules d'écriture et les fournisseurs. Après la création d'une copie miroir de sauvegarde, VSS en informe Data Protector. Data Protector effectue une sauvegarde à partir du volume de copie miroir sur le support, puis indique à VSS que la copie miroir peut être extraite.

## Restauration VSS

La restauration d'intégration VSS fait référence à la restauration des données qui ont été sauvegardées à l'aide de Volume Shadow Copy Service et d'un module d'écriture. Pendant la procédure de restauration, Volume Shadow Copy Service coordonne les communications entre Data Protector et les modules d'écriture.

Lors de la restauration de modules d'écriture VSS, Data Protector restaure d'abord toutes les métadonnées pertinentes afin d'identifier les composants de sauvegarde et de déterminer la méthode de restauration. Il se connecte ensuite à Volume Shadow Copy Service et indique que la restauration est sur le point de commencer. VSS coordonne les activités des modules d'écriture pendant la restauration. Une fois que Data Protector a correctement restauré les données, VSS indique aux modules d'écriture que la restauration est terminée ; les modules d'écriture peuvent alors accéder aux données restaurées et commencer leur traitement en interne.

# Sauvegarde et restauration de système de fichiers VSS

Certaines applications ne détectent pas la présence de Volume Shadow Copy Service. Ces applications ne peuvent pas garantir la cohérence des données lors de la création d'une copie miroir. Le mécanisme VSS n'est pas en mesure de coordonner les activités de ces applications afin d'effectuer une sauvegarde cohérente.

Vous pouvez malgré tout bénéficier de la fonctionnalité VSS. La coopération entre l'application de sauvegarde et un fournisseur de copies miroir peut quand même être utilisée pour garantir la plus grande cohérence possible des données. Microsoft

utilise le terme “cohérence des données en cas de panne” pour qualifier cet état des données. Dans ce cas, le mécanisme VSS réalise toutes les opérations d'E/S en attente et interrompt les demandes d'écriture entrantes pendant la préparation d'un volume de copie miroir. Ainsi, tous les fichiers du système de fichiers sont fermés et déverrouillés pendant la création de la copie miroir.

La fonctionnalité Microsoft Volume Shadow Copy permet de créer des copies miroir de volumes sans l'intervention des applications en cours de sauvegarde. Dans ce cas, le volume de copie miroir est créé, puis sauvegardé par Data Protector. Cette démarche peut être utilisée avec les applications qui ne détectent pas le mécanisme VSS.

---

❗ **IMPORTANT :**

Lors de la sauvegarde d'applications qui ne détectent pas le mécanisme VSS, la cohérence des données du point de vue des applications ne peut être garantie. Dans ce cas, elle est la même qu'en cas de panne d'alimentation. Data Protector ne peut garantir la cohérence des données lorsque les applications ne participent pas activement à la création d'une copie miroir.

---

Lors de la sauvegarde d'un système de fichiers VSS, la cohérence des données est supérieure à celle que fournirait la sauvegarde d'un système de fichiers non-VSS. VSS vous permet de créer des sauvegardes de volumes par copie miroir et des copies exactes de fichiers à un moment donné (y compris tous les fichiers ouverts). Par exemple, les bases de données qui restent ouvertes exclusivement et les fichiers ouverts en raison de l'activité de l'opérateur ou du système sont sauvegardés en cas de sauvegarde de système de fichiers VSS. Ainsi, les fichiers qui ont été modifiés pendant la procédure de sauvegarde sont correctement copiés.

La sauvegarde d'un système de fichiers VSS présente les avantages suivants :

- Il est possible de sauvegarder un ordinateur pendant que des applications et des services sont en cours d'exécution. Par conséquent, les applications peuvent continuer à écrire des données sur le volume pendant une sauvegarde.
- Les fichiers ouverts ne sont plus ignorés pendant la sauvegarde, car ils apparaissent fermés sur le volume de copie miroir au moment de la création de la copie miroir.
- Les sauvegardes peuvent être effectuées à tout moment sans obliger les utilisateurs à arrêter leur système.
- De plus, l'incidence d'une sauvegarde sur les performances du système d'application est minime, voire nulle.

## Sauvegarde et restauration

La sauvegarde VSS est mise en oeuvre comme une sauvegarde supplémentaire du système de fichiers Windows sous Windows Server 2003 et sur tous les systèmes d'exploitation Windows plus récents. Le niveau d'intégrité des données est légèrement supérieur à celui obtenu lors d'une sauvegarde traditionnelle d'un volume actif. Pour obtenir des informations détaillées sur la sauvegarde et la restauration de système de fichiers Windows, reportez-vous à l'aide en ligne.

Au cours de la sauvegarde d'un système de fichiers VSS, les applications ne peuvent contribuer à la cohérence des données puisqu'elles ne détectent pas le mécanisme VSS. Toutefois, Data Protector et un fournisseur peuvent toujours coopérer pour créer des copies miroir des volumes. La sauvegarde d'un système de fichiers VSS permet de sauvegarder les données telles qu'elles apparaissent à un moment donné, quelle que soit l'activité d'E/S du système pendant la sauvegarde.

Lorsque Data Protector demande la sauvegarde des volumes spécifiés dans la spécification de sauvegarde, le mécanisme VSS réalise toutes les opérations d'E/S en attente, interrompt les demandes d'écriture entrantes et prépare un volume de copie miroir.

Lorsque la copie miroir est créée, Data Protector lance sa procédure de sauvegarde normale, si ce n'est que le volume source est remplacé par la copie miroir qui vient d'être créée. En cas d'échec de la création de la copie miroir, Data Protector poursuit la sauvegarde normale du système de fichiers si ce comportement a été défini dans la spécification de sauvegarde.

Il est ainsi possible de sauvegarder un ordinateur pendant que des fichiers sont ouverts et des services en cours d'exécution. Les fichiers ne sont pas ignorés pendant ce type de sauvegarde. VSS permet aux services et aux applications de continuer à fonctionner sans interruption sur les volumes réels pendant la création d'une copie miroir. Une fois la sauvegarde terminée, la copie miroir est supprimée.

La restauration de données sauvegardées à l'aide de la sauvegarde de système de fichiers VSS est similaire à la procédure de restauration standard.



### REMARQUE :

Vous pouvez également utiliser des modules d'écriture VSS pour effectuer une sauvegarde d'image disque en définissant les variables `omnirc`.

---



---

# A Scénarios de sauvegarde

## Dans cette annexe

Cette annexe décrit deux scénarios : l'un pour l'entreprise XYZ, l'autre pour l'entreprise ABC. Ces deux entreprises souhaitent améliorer leurs systèmes de stockage de données. Leurs solutions de sauvegarde actuelles sont décrites ainsi que les problèmes qu'elles présentent. Des solutions sont ensuite proposées pour remédier à ces problèmes et répondre aux besoins futurs de ces entreprises en matière de stockage de données.

## Éléments à prendre en considération

Dans les deux cas, les éléments suivants sont à prendre en compte pour formuler la stratégie de sauvegarde de l'entreprise :

- Importance de la disponibilité des données du système (et de la sauvegarde) pour l'entreprise :
  - Nécessité de conserver les données sauvegardées à un emplacement distant en cas de sinistre.
  - Niveau de continuité des opérations, comprenant notamment un plan de récupération et de restauration pour l'ensemble des systèmes stratégiques.
  - Sécurité des données sauvegardées  
Nécessité de contrôler l'accès aux locaux, afin d'en interdire l'entrée à toute personne non autorisée. Cela comprend également la protection des données pertinentes contre tout accès non autorisé, à l'aide de dispositifs physiques empêchant d'y accéder et d'une protection électronique par mot de passe.
- Types de données à sauvegarder :  
Vous pouvez regrouper les données en catégories, telles que Données commerciales, Données de ressources de l'entreprise, Données de projet et Données personnelles, chaque catégorie ayant des besoins spécifiques.
- Facteurs de performance pour la sauvegarde et la restauration :

- Topologie réseau et système  
Déterminez quels systèmes peuvent utiliser quels liens réseau, et quels taux de transfert sont possibles.
- Fenêtre temporelle  
Définissez les périodes au cours desquelles les sauvegardes de systèmes spécifiques peuvent être effectuées.
- Sauvegardes locales ou réseau  
Parmi les systèmes auxquels sont connectés des périphériques de sauvegarde, déterminez lesquels seront sauvegardés en local et lesquels seront sauvegardés sur le réseau.
- Mise en œuvre de la stratégie de sauvegarde :
  - Comment les sauvegardes sont-elles effectuées et quelles sont les options de sauvegarde utilisées ?  
Ces critères permettent de définir la fréquence des sauvegardes complètes et incrémentales, les options de sauvegarde à utiliser, et si les données sauvegardées doivent ou non être protégées définitivement à l'aide de supports stockés sur un site distant.
  - Comment regrouper les systèmes dans des spécifications de sauvegarde ?  
Étudiez la meilleure manière de regrouper les spécifications de sauvegarde (par service, par type de données ou par fréquence de sauvegarde).
  - Comment planifier les sauvegardes ?  
Pensez à utiliser une approche échelonnée, selon laquelle les sauvegardes complètes des divers clients (spécifications de sauvegarde) se déroulent à des dates différentes afin d'éviter les problèmes liés à une surcharge du réseau, à une surcharge des périphériques et à la fenêtre temporelle.
  - Comment conserver les données stockées sur les supports et les informations concernant les sauvegardes ?  
Pensez à protéger les données pendant une période spécifique contre tout risque d'écrasement lors de nouvelles sauvegardes.  
Définissez la période à laquelle la base de données catalogue Data Protector doit stocker les informations sur les sauvegardes.
- Configuration des périphériques  
Déterminez les périphériques à utiliser pour les sauvegardes et les systèmes auxquels ils sont connectés. Connectez les périphériques de sauvegarde aux systèmes comportant les plus grandes quantités de données, afin de sauvegarder le plus de données possibles localement plutôt que via le réseau. Vous accélérez ainsi la vitesse de sauvegarde.

Si vous devez sauvegarder de grandes quantités de données, pensez à utiliser un périphérique de bibliothèque.

- Gestion des supports  
Déterminez le type de support à utiliser, ainsi que la manière de regrouper les supports en pools et de placer les objets sur ces supports.
- Mise au coffre  
Décidez si les supports doivent être stockés en lieu sûr, où ils seront conservés durant une période déterminée.
- Administrateurs et opérateurs de sauvegarde  
Définissez les droits d'administration et d'accès pour les utilisateurs des systèmes de sauvegarde.

## Entreprise XYZ

XYZ est une agence de traduction proposant les services suivants :

- Traduction, localisation, adaptation linguistique et relecture
- Certification de documents traduits
- Interprétation consécutive et simultanée
- Publication et graphisme assistés par ordinateur
- Location de matériel pour l'interprétation de conférence

La croissance annuelle de XYZ se situe actuellement entre 20 et 25 %, mais sa solution de sauvegarde n'est pas adaptée au rythme de cette croissance. Le processus de sauvegarde requiert l'intervention d'un personnel nombreux, car les bandes de sauvegarde doivent être gérées manuellement.

## Environnement

Cette section décrit l'environnement matériel et logiciel actuel de XYZ, et la manière dont est mise en œuvre la stratégie de stockage des données.

XYZ est divisée en trois services connectés à un réseau d'entreprise principal :

- Le service Anglais
- Le service Autres langues
- Le service Administration

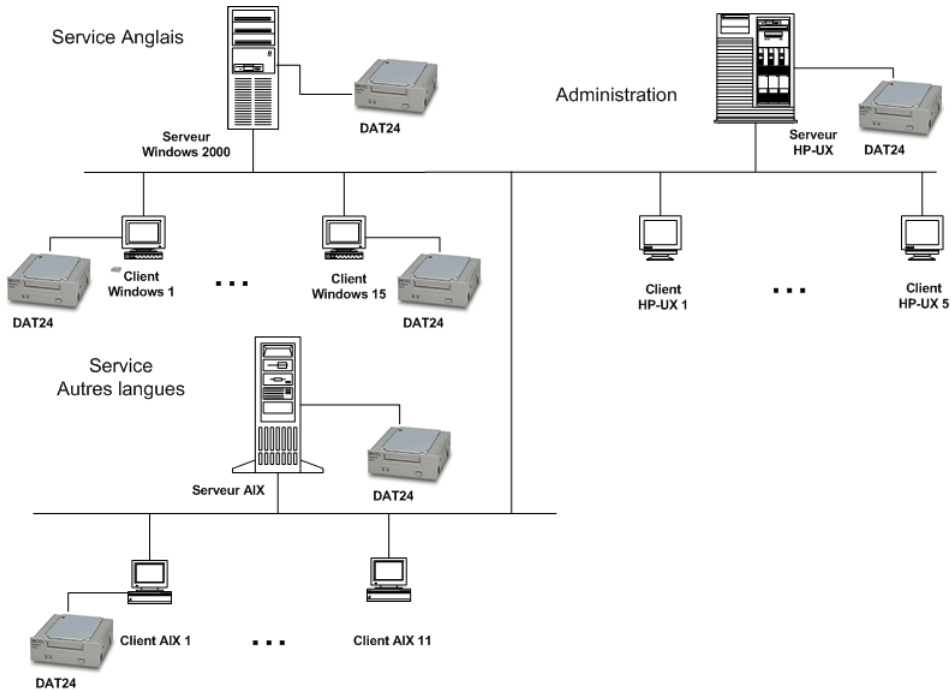
Vous trouverez la description de l'environnement matériel et logiciel d'XYZ dans le [Tableau 15](#) à la page 320, et celle de sa topologie de sauvegarde actuelle à la [Figure 84](#) à la page 321.

**Tableau 15 Environnement matériel et logiciel de XYZ**

Service	Nb de serveurs	Nb de clients	Qté de données actuelle	Qté de données prévue (dans 5 ans)	Périphériques actuels
Anglais	1 Windows	15 Windows	35 Go	107 Go	3 chargeurs automatiques HP StorageWorks DAT24
Autres langues	1 AIX	11 UX	22 Go	67 Go	2 chargeurs automatiques HP StorageWorks DAT24
Admin	1 HP-UX	5 UX	10 Go	31 Go	1 chargeur automatique HP StorageWorks DAT24

La [Figure 84](#) à la page 321 présente l'organisation de l'environnement de sauvegarde de XYZ.





**Figure 84 Topologie de sauvegarde actuelle de XYZ**

XYZ dispose actuellement de trois serveurs pour un volume de données total estimé à 67 Go. Dans le service Anglais, chaque employé copie manuellement les données tous les soirs sur son serveur respectif. L'un des clients Windows de ce service stocke environ un tiers des données (12 Go).

La sauvegarde des systèmes clients du service Autres langues s'effectue via un NFS (Network File System), tandis que celle des systèmes client du service Administration s'effectue par le biais de partages réseau. Les employés du service Autres langues travaillent également le samedi.

### Problèmes rencontrés avec la solution actuelle

La solution de sauvegarde actuelle n'est pas adaptée au rythme de la croissance de XYZ. Le processus de sauvegarde actuel nécessite beaucoup de travail manuel. Il ne permet pas d'améliorer la gestion de la sauvegarde ni d'installer une architecture de sauvegarde unique pour l'ensemble de l'entreprise. Chacun des serveurs de sauvegarde est géré séparément. Il est impossible de centraliser la gestion de sauvegarde. Voici quelques-uns des problèmes liés à la solution actuelle :

- La solution de sauvegarde n'est pas automatisée.

- Les employés doivent copier leur travail régulièrement, ce qui augmente les risques d'erreur.
- Les utilitaires de sauvegarde ne sont pas les mêmes, ce qui entraîne un accroissement des coûts de formation.
- Les solutions utilisées dans le service Autres langues et le service Administration sont plus élaborées mais présentent également des problèmes spécifiques. L'utilisation du réseau influe considérablement sur les performances de sauvegarde. De plus, toutes les données ne sont pas sauvegardées. Seuls les fichiers partagés via le Network File System sont sauvegardés dans le service Autres langues, et seuls les fichiers partagés sur réseau sont sauvegardés dans le service Administration.
- Les trois services utilisant chacun un serveur de sauvegarde indépendant, il n'y a pas de centralisation du contrôle ni de la gestion des opérations clés suivantes :
  - Configuration des périphériques
  - Gestion des supports
  - Configuration de sauvegarde
  - Programmation
  - Surveillance
  - Opérations de restauration
- Chaque serveur de sauvegarde étant géré individuellement, la génération des rapports n'est pas centralisée.
- La solution actuelle n'offre aucune fonction de récupération après sinistre, ce qui constitue un inconvénient de plus en plus important. En effet, un sinistre peut entraîner la perte d'une partie essentielle du travail de l'entreprise.

## Besoins relatifs à une stratégie de sauvegarde

### Besoins

Après avoir pris en compte les éléments énumérés à la section “[Éléments à prendre en considération](#)” à la page 317, nous avons identifié les besoins suivants pour la solution de sauvegarde de l'entreprise XYZ :

- Stratégie de sauvegarde :
  - Des sauvegardes hebdomadaires complètes seront réalisées en l'espace de 12 heures.
  - Des sauvegardes incrémentales quotidiennes seront réalisées en l'espace de 8 heures à la fin de chaque journée de travail.
  - Une période fixe pour la protection des données sera mise en place.

- Les supports de sauvegarde seront stockés sur un site distant.
- Sauvegarde  
Toutes les opérations de sauvegarde doivent nécessiter moins d'intervention manuelle qu'actuellement.
- Restauration
  - Une restauration pratique et rapide doit être proposée. Les données à restaurer doivent pouvoir être explorées pendant les trois semaines suivant la sauvegarde.
  - La restauration des sauvegardes de données placées dans le coffre doit être possible en deux jours.
- Connexion réseau :  
Les serveurs de sauvegarde et les services seront connectés à un réseau local Ethernet 100TX.
- Croissance prévue :  
On prévoit 20 à 25 % d'augmentation annuelle des capacités de données pour les cinq années à venir.
- Logiciels :  
Les serveurs de sauvegarde doivent s'exécuter sur l'un des systèmes d'exploitation pris en charge. Pour obtenir des informations sur les systèmes d'exploitation pris en charge pour le Gestionnaire de cellule, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Protection contre un sinistre :  
Une fois les sauvegardes terminées, les supports seront stockés sur site où ils pourront être récupérés à la demande pour la restauration de fichiers. Au bout de 20 jours, ils seront déplacés vers un lieu de stockage hors site afin d'être protégés en cas de sinistre dans l'entreprise, et afin de libérer de la place pour de nouveaux supports de sauvegarde.

## Solution proposée

Etant donné les performances limitées de la solution actuelle et l'impossibilité d'une gestion centralisée, XYZ doit revoir la conception de son architecture et de sa stratégie de sauvegarde afin de pouvoir atteindre ses objectifs commerciaux. La solution proposée est d'abord présentée dans son ensemble, puis en détails. Notez qu'il s'agit d'une proposition et non de la seule solution possible aux problèmes de gestion de stockage de l'entreprise XYZ.

## Présentation générale de la solution

Tous les clients et serveurs doivent être configurés dans une seule cellule Data Protector avec le serveur Windows du service Anglais, utilisé à la fois comme Gestionnaire de cellule et comme Serveur d'installation pour les systèmes Windows. Utilisez le serveur de sauvegarde HP-UX du service Administration comme Serveur d'installation pour les systèmes UNIX. Les périphériques de sauvegarde sont les suivants: une bibliothèque HP StorageWorks DLT 4115w et deux des chargeurs automatiques HP StorageWorks DAT24 utilisés jusqu'à présent. Ce matériel est suffisant pour les cinq années à venir au taux de croissance actuel de 20 à 25 % par an. L'utilisation de périphériques existants constitue un avantage supplémentaire dans le cas d'une récupération après sinistre. Le client Windows, qui comporte environ un tiers des données du service Anglais (12 Go), doit être sauvegardé en local sur un chargeur automatique HP StorageWorks DAT24. La solution de sauvegarde proposée offre les avantages suivants :

- Sauvegardes très performantes
- Gestion des supports avec intervention minimale du personnel
- Récupération après sinistre simple et efficace
- Génération centralisée de rapports sur les sauvegardes
- Automatisation de la plupart des opérations de sauvegarde

Toutes ces opérations sont réalisées avec une seule solution, en association avec le matériel proposé :

**Tableau 16 Environnement proposé**

Service	Qté de données actuelle	Qté de données prévue (dans 5 ans)	Périphériques	
Anglais*	35 Go	107 Go	Bibliothèque HP DLT 4115	2 chargeurs automatiques HP StorageWorks DAT24
Autres langues	22 Go	67 Go		
Admin	10 Go	31 Go		
* Un chargeur automatique HP StorageWorks DAT24 est actuellement utilisé pour sauvegarder en local les 12 Go de données. L'autre chargeur automatique HP StorageWorks DAT24 est utilisé pour sauvegarder les fichiers de configuration et la base de données IDB. Les autres données du service sont sauvegardées à distance vers la bibliothèque HP StorageWorks DLT 4115.				

Les quatre autres chargeurs automatiques HP StorageWorks DAT24 sont utilisés sur un système R&D. séparé qui n'est pas intégré à la configuration proposée.

L'un des composants logiciels proposés pour la solution de sauvegarde d'entreprise est HP Data Protector 6.20.

### Description détaillée de la solution proposée

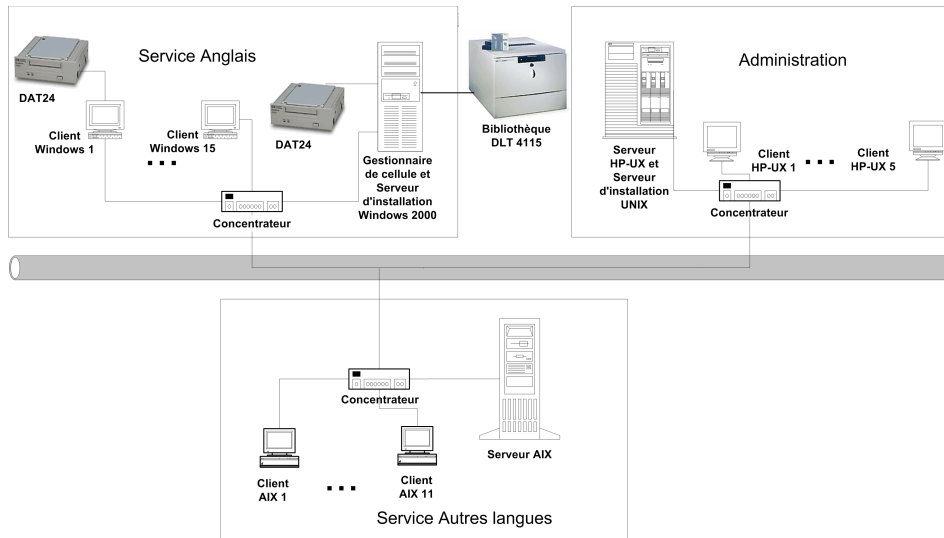
La solution proposée est décrite en détail ci-dessous :

- Configuration de la cellule :

Tous les clients et serveurs doivent être configurés dans une seule cellule Data Protector. Le Gestionnaire de cellule Data Protector peut fonctionner sur le serveur Windows du service Anglais.

Pour des performances optimales, tous les systèmes de la cellule doivent se trouver sur le même réseau local. Le Gestionnaire de cellule doit également être utilisé comme Serveur d'installation pour Windows. Utilisez le serveur de sauvegarde HP-UX du service Administration comme Serveur d'installation pour UNIX. La bibliothèque HP StorageWorks DLT 4115w doit être connectée au Gestionnaire de cellule, de même qu'un chargeur automatique HP StorageWorks DAT24 pour la sauvegarde des fichiers de configuration et de la base de données IDB. Le client Windows, qui stocke environ un tiers des données du service Anglais (12 Go), doit être sauvegardé en local sur un chargeur automatique HP StorageWorks DAT24.

L'environnement de sauvegarde proposé est illustré par la [Figure 85](#) à la page 326 :



**Figure 85 Topologie de sauvegarde proposée pour XYZ**

- Le Gestionnaire de cellule gère la base de données catalogue (CDB). Cela permet de disposer pendant au moins 20 jours du détail des fichiers et des répertoires dans la base de données en cours.

#### Estimation de la taille de la base de données IDB

L'outil de planification de capacité de la base de données interne a été utilisé pour estimer la taille atteinte par la base de données IDB en une année. Cet outil est situé dans le même répertoire que les autres manuels Data Protector en ligne. Les paramètres d'entrée présentés à la [Figure 86](#) à la page 327 comprennent le nombre de fichiers dans l'environnement (2 millions), le facteur de croissance (1,2), la protection des données (52 semaines), la protection de catalogue (3 semaines), le nombre de sauvegardes complètes hebdomadaires (1) et le nombre de sauvegardes incrémentales hebdomadaires (5).

<b>Description de l'environnement</b>	Fichiers :	2	millions
	Fichiers par répertoire :	10	
	Volume de données :	200	Go
	Facteur de croissance :	1,20	
	Performances du périph. :	10,00	Mo/s
	Capacité du support :	70,00	Go
	Objets :	50	
	Modif. par sauv. incrément. :	5,00%	
<b>Paramètres de sauvegarde</b>			
	Périphériques simult. :	2	
	Taille segment données :	2048,00	Mo
	Niveau de journalisation :	Tout	
	Protection des données :	52	semaines
	Protection du catalogue :	3	semaines
	Sauv. complètes/semaine :	1	
	Sauv. incrémentielles/sem. :	5	
<b>Param. du Gestionnaire de cellule</b>			
	Vitesse d'insertion :	12	millions/h

**Figure 86 Paramètres d'entrée**

Les résultats sont présentés à la [Figure 87](#) à la page 327. En une année, la base de données devrait croître pour atteindre environ 419,75 Mo.

<b>Résultats/calculs</b>			
	Taille de fichier moy. :	123,36	Ko
	Fichiers/segment :	16931,38	
	Taille de catalogue :	1,03	Mo
	Périphériques K :	40	
	Performances K :	1445,647059	Go/h
	Durée K :	0,14	heure
	Supports protégés :	278,5714286	
<b>Estimation espace</b>			
	MMDB :	30,00	Mo
CDB :	Enames :	153,00	Mo
	Overs :	5,71	Mo
	Mpos :	1,54	Mo
DCBF :		229,50	Mo
SMBF :		2,86	Mo
Total :		419,75	Mo

**Figure 87 Résultats**

- Matériel
  - Réseau

Pour des performances optimales, l'ensemble des systèmes doit se trouver sur le même réseau 100TX. Ce réseau présente un taux de transfert de données de 10 Mo/s ou 36 Go/h.

- Périphériques de sauvegarde

Les périphériques de sauvegarde sont les suivants : une bibliothèque HP StorageWorks DLT 4115w et deux chargeurs automatiques HP StorageWorks DAT24.

**Pourquoi utiliser la bibliothèque HP StorageWorks DLT 4115w ?**

La bibliothèque HP StorageWorks DLT 4115w est dotée d'un seul lecteur DLT4000 avec 15 emplacements. Elle présente une capacité totale de stockage compressé de 600 Go et un taux de transfert maximum de 3 Mo/s, ou 10,5 Go/h, avec compression de données. Il s'agit du taux sur lequel nous nous baserons pour la suite de cette section. Actuellement, la quantité totale de données à sauvegarder vers la bibliothèque HP StorageWorks DLT 4115w dans le cadre d'une sauvegarde complète, qu'il s'agisse d'une seule sauvegarde ou d'une planification répartie, est d'environ 55 Go. En supposant que la taille d'une sauvegarde incrémentale corresponde à environ 5 % de celle d'une sauvegarde complète, une génération de sauvegarde, c'est-à-dire une sauvegarde complète plus toutes les sauvegardes incrémentales qui en découlent, nécessite un espace de  $(55 + 55 * 5 \% * 5)$  Go, soit **68,75 Go**, dans la bibliothèque. D'ici cinq ans, cet espace nécessaire devrait augmenter pour atteindre environ 210 Go. La stratégie de sauvegarde d'XYZ nécessite la conservation de deux générations de sauvegarde de données. Un espace de  $210 \times 2$  Go, soit 420 Go, est donc nécessaire dans la bibliothèque pour le stockage. La capacité de stockage (600 Go) de la bibliothèque HP StorageWorks DLT 4115w est donc suffisante.

**Pourquoi utiliser le chargeur automatique HP StorageWorks DAT24 ?**

Le chargeur automatique HP StorageWorks DAT24 est doté de six cartouches de données de 24 Go. Il présente une capacité totale de stockage compressé de 144 Go et un taux de transfert maximum de 2 Mo/s, ou 7 Go/h, avec compression de données. Il s'agit du taux sur lequel nous nous baserons pour la suite de cette section. Actuellement, la quantité totale de données à sauvegarder vers le chargeur automatique HP StorageWorks DAT24 (connecté au client Windows du service Anglais mentionné plus haut) dans le cadre d'une seule sauvegarde complète est de 12 Go. En supposant que la taille d'une sauvegarde incrémentale corresponde à environ 5 % de celle d'une sauvegarde complète, une génération de sauvegarde, c'est-à-dire une sauvegarde complète plus toutes les sauvegardes incrémentales qui en découlent, nécessite un espace de  $(12 + 12 * 5 \% * 5)$  Go, soit **15 Go**. D'ici cinq ans, cet espace nécessaire devrait augmenter pour atteindre environ 45 Go. La stratégie de sauvegarde d'XYZ nécessite la conservation de deux générations de sauvegarde de données. Un espace de  $45 \times 2$  Go, soit **90 Go**, est donc nécessaire dans la bibliothèque pour le stockage. La capacité de stockage (144 Go) du chargeur automatique HP StorageWorks DAT24 est donc suffisante.



## Combien de temps dure une sauvegarde complète ?

Le client Windows du service Anglais, sur lequel sont stockés 12 Go de données, doit être sauvegardé en local sur un chargeur automatique HP StorageWorks DAT24. Ce périphérique présente un taux de transfert de données de 2 Mo/s ou 7 Go/h environ. Par conséquent, la sauvegarde complète de ce client Windows prend environ **2 heures**. La quantité de données augmentant de 20 à 25 % par an, il est prévu que ce client contienne environ 36 Go de données dans cinq ans. La sauvegarde de ces données prendrait alors **6 heures**.

La base de données catalogue Data Protector a une taille d'environ 0,4 Go. Elle est sauvegardée en local sur un chargeur automatique HP StorageWorks DAT24 dont le taux de transfert de données est de 2 Mo/s, ou 7 Go/h. Par défaut, Data Protector vérifie l'intégrité de la base de données avant sa sauvegarde. La vérification de l'intégrité d'une base de données de 0,4 Go prend moins d'une demi-heure, et sa sauvegarde seulement quelques minutes. Ainsi, le processus de vérification et de sauvegarde de la base de données IDB et des fichiers de configuration dure moins d'**une heure**.

Dans cinq ans, la taille de la base de données devrait atteindre 1,2 Go. La vérification de l'intégrité d'une base de données de 1,2 Go prend moins d'une heure, et sa sauvegarde moins d'une demi-heure. Ainsi, le processus de vérification et de sauvegarde de la base de données IDB et des fichiers de configuration dure moins de **2 heures**.

Toutes les autres données disponibles du système (représentant actuellement 55 Go environ) sont sauvegardées à distance vers la bibliothèque HP StorageWorks DLT 4115w, dont le taux de transfert de données supporté est de 3 Mo/s ou 10,5 Go/h. La plupart de ces données passent par le réseau 100TX, dont le taux de transfert de données supporté est de 10 Mo/s ou 36 Go/h. Il n'y a pas de goulet d'étranglement. La sauvegarde de toutes ces données devrait donc prendre entre **5 et 7 heures** environ, ce qui est inférieur aux 12 heures autorisées. Un problème se pose toutefois : lorsque les données atteindront 170 Go comme prévu dans cinq ans, la sauvegarde durera entre 15 et 21 heures !

Pour remédier à ce problème, adoptez la planification répartie. Planifiez la sauvegarde complète des données du service Anglais pour chaque vendredi à 20:00, celle des données du service Autres langues pour chaque samedi à 20:00 et celle des données du service Administration pour chaque dimanche à 20:00.

**Tableau 17** Planification répartie

	Lun	Mar	Mer	Jeu	Ven	Sam	Dim
--	-----	-----	-----	-----	-----	-----	-----

Anglais	Incr. 1	Incr. 1	Incr. 1	Incr. 1	Complète	Incr. 1	
Autres langues	Incr. 1	Incr. 1	Incr. 1	Incr. 1	Incr. 1	Complète	
Admin	Incr. 1	Incr. 1	Incr. 1	Incr. 1	Incr. 1		Complète

Le [Tableau 18](#) à la page 330 présente les caractéristiques en matière de quantité de données et de durée pour les sauvegardes complètes effectuées aujourd'hui, ainsi que pour celles effectuées d'ici à cinq ans.

**Tableau 18 Sauvegardes complètes à distance vers la bibliothèque HP DLT 4115**

Service	Qté de données actuelle/Durée de la sauvegarde	Données prévues/Durée de la sauvegarde
Anglais	23 Go / 3 h	70 Go / 7 h
Autres langues	22 Go / 3 h	67 Go / 7 h
Admin	10 Go / 1 h	31 Go / 3 h

En supposant que la taille d'une sauvegarde incrémentale corresponde à 5 % de celle d'une sauvegarde complète, la durée pour une sauvegarde complète de toutes les données sauvegardées à distance dans le service le plus important (Anglais), ainsi que des sauvegardes incrémentales des deux autres services, devrait atteindre dans cinq ans  $7 + 5\%$  ( $7 + 0,35$ ) heures, soit à moins de 8 heures, ce qui est inférieur aux 12 heures autorisées.

- Pools de supports

Les supports sont regroupés dans des pools pour être mieux suivis et contrôlés. Regroupez les supports du même type (DLT ou DDS) dans leurs pools respectifs.

- DDS par défaut

Ce pool doit être utilisé pour tous les supports DDS.

- DLT par défaut

Ce pool doit être utilisé pour tous les supports DLT.

- DB\_Pool

Ce pool doit être utilisé pour les fichiers de configuration et la base de données IDB. Pour des raisons de sécurité, il est recommandé de sauvegarder la base de données sur deux supports.

- Spécifications de sauvegarde

Configurez cinq spécifications de sauvegarde, une pour chaque service, et une pour les fichiers de configuration et la base de données IDB :

- ENG1\_BS

Spécification de sauvegarde pour le client Windows à sauvegarder en local dans le service Anglais. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète chaque vendredi et une sauvegarde incrémentale de niveau 1 tous les jours à 20:00, sauf le vendredi et le dimanche.

### Pourquoi utiliser des sauvegardes incrémentales de niveau 1 ?

Pour restaurer les données les plus récentes, seuls deux jeux de supports sont nécessaires : l'un pour la dernière sauvegarde complète et l'autre pour la dernière sauvegarde incrémentale de niveau 1 précédant la restauration. Cela permet de simplifier et d'accélérer considérablement le processus de restauration.

- ENG2\_BS

Spécification de sauvegarde pour les données du service Anglais devant être sauvegardées à distance vers la bibliothèque HP StorageWorks DLT 4115w. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète chaque vendredi et des sauvegardes incrémentales de niveau 1 tous les jours à 20:00, sauf le dimanche.

- OTH\_BS

Spécification de sauvegarde pour les données du service Autres langues devant être sauvegardées à distance vers la bibliothèque HP StorageWorks DLT 4115w. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète chaque samedi à 20:00 et des sauvegardes incrémentales de niveau 1 tous les jours à 20:00, sauf le dimanche.

- ADM\_BS

Spécification de sauvegarde pour les données du service Admin devant être sauvegardées à distance vers la bibliothèque HP StorageWorks DLT 4115w. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète chaque dimanche à 20:00 et des sauvegardes incrémentales de niveau 1 tous les jours à 20:00, sauf le samedi.

- DB\_BS

Spécification de sauvegarde pour les fichiers de configuration et la base de données IDB. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète tous les jours à 04:00. A cette

heure, les autres sauvegardes complètes et incrémentales seront terminées et aucun problème lié au partage des ressources processeur ne se présentera entre le Gestionnaire de cellule et les autres systèmes client. Il est recommandé de faire deux copies de la base de données.

## Options de sauvegarde

- Utilisez les options de sauvegarde Data Protector par défaut. Définissez les options comme suit :
  - Protection du catalogue  
La protection de catalogue permet de définir l'intervalle de temps au cours duquel la base de données catalogue Data Protector doit conserver les informations sur les versions sauvegardées, sur le nombre de fichiers et de répertoires sauvegardés et sur les messages stockés dans la base de données. A l'expiration de la protection de catalogue, il n'est plus possible d'explorer les fichiers et répertoires à l'aide de l'interface Data Protector. Choisissez une protection de 20 jours.
  - Protection de données  
La protection des données détermine l'intervalle de temps au cours duquel un support ne peut pas être réutilisé. Choisissez une protection des données permanente afin de vous assurer que les données figurant sur les supports ne soient pas écrasées involontairement.
  - Simultanéité  
Définissez à 5 le nombre d'Agents de disque pouvant écrire en même temps des données dans la bibliothèque HP StorageWorks DLT 4115w. Vous améliorerez ainsi les performances de sauvegarde.
  - Pool de supports  
Pour la base de données IDB, sélectionnez le pool DB\_Pool contenant les supports appropriés à utiliser. Pour d'autres objets, utilisez les pools de supports par défaut.

## Options de restauration

- Utilisez les options de restauration Data Protector par défaut. Définissez les options comme suit :
  - Lister fichiers restaurés  
Activez cette option pour obtenir la liste des chemins d'accès des fichiers et répertoires restaurés. Lorsque les fichiers à restaurer sont trop nombreux, cette opération peut ralentir la procédure de restauration.

- Afficher statistiques

Activez cette option pour afficher les statistiques détaillées sur une session de restauration particulière, notamment le nombre de fichiers et de répertoires restaurés et la quantité de données restaurées.

- Génération de rapports et notifications

Des notifications envoyées par e-mail aux administrateurs de sauvegarde sont définies pour les demandes de montage, en cas d'espace insuffisant dans la base de données, en cas d'erreurs de périphériques et à la fin des sessions pour toutes les spécifications de sauvegarde. Eventuellement, des notifications par e-mail ou message de diffusion sont définies pour les utilisateurs finaux souhaitant être informés de la réussite des sauvegardes de leurs systèmes.

Pour permettre à tous les utilisateurs de connaître facilement l'état de leurs sauvegardes, définissez les informations de sauvegarde client sur l'Intranet de l'entreprise comme suit :

1. Configurez un groupe de rapports avec un rapport sur la sauvegarde client pour chaque client. Le rapport doit être enregistré dans le fichier au format HTML.
2. Planifiez le groupe de rapports.
3. Reliez les fichiers contenant les rapports à la page Intranet de l'entreprise.

- Mise au coffre

La mise au coffre consiste à stocker des supports en lieu sûr pendant une période déterminée.

Des supports seront déplacés vers le coffre une fois par semaine, et remplacés par de nouveaux supports dans la bibliothèque HP StorageWorks DLT 4115w et les chargeurs automatiques HP StorageWorks DAT24. Toutes les actions, hormis le déplacement de supports vers le coffre, sont exécutées par la solution logicielle, y compris les requêtes effectuées en interne dans la base de données pour éviter à l'administrateur d'avoir à rechercher les supports devant être éjectés.

Le second déplacement des supports s'effectue du coffre vers une entreprise de sécurité. Celui-ci a lieu une fois par mois. Data Protector publie un rapport sur les supports devant être déplacés vers l'entreprise de sécurité.

Effectuez le suivi des supports déplacés vers un coffre. Cette opération est utile lorsque vous souhaitez restaurer des données à partir de sauvegardes réalisées sur un support déplacé vers une entreprise de sécurité. Data Protector vous permet d'effectuer les tâches de mise au coffre suivantes :

- Génération de rapports sur les supports stockés à un endroit spécifique et dont la protection des données expire à une date déterminée

- Génération de rapports sur les supports utilisés pour une sauvegarde au cours d'une période donnée
- Affichage d'une liste de spécifications de sauvegarde ayant utilisé des supports spécifiques lors de la sauvegarde
- Affichage d'une liste de supports nécessaires pour les opérations de restauration et des emplacements physiques où sont stockés ces supports
- Filtrage des supports à partir de l'affichage des supports selon des critères spécifiques (affichage des supports dont la protection a expiré, par exemple)
- Restauration
  - Restaurer par requête
 

Les demandes de restauration par requête sont envoyées à l'administrateur. Si la dernière sauvegarde des fichiers date de moins de 20 jours avant l'émission de la requête, l'administrateur peut utiliser l'option Restaurer par requête pour sélectionner les fichiers et répertoires à restaurer selon des critères particuliers. Il choisit ensuite l'option Ecraser pour remplacer les fichiers et répertoires du disque par les versions figurant sur le support.
  - Restauration complète de système de fichiers
 

Les demandes de restauration de systèmes de fichiers entiers sont envoyées à l'administrateur. Si la dernière sauvegarde des fichiers date de moins de 20 jours avant l'émission de la requête, l'administrateur peut sélectionner les objets à restaurer et utiliser l'option Restaurer dans.

Les objets sont alors restaurés avec la même structure de répertoires dans un répertoire sélectionné. Servez-vous d'un utilitaire Windows ou UNIX pour comparer les objets restaurés aux objets sauvegardés.
  - Restauration à partir d'un coffre
 

Pour restaurer des données à partir d'un coffre (sauvegardées, par exemple, 3 ans auparavant), envoyez une requête à l'administrateur. Celui-ci effectue alors les opérations suivantes :

    1. Il identifie les supports nécessaires à la restauration.
    2. Il déplace les supports du coffre vers la bibliothèque HP StorageWorks DLT 4115w ou vers un autre périphérique, puis les analyse.
    3. Si le support ne se trouve pas dans la base de données IDB, il sélectionne l'objet spécifique à restaurer à l'aide de l'option Lister depuis supports.
    4. Il effectue la restauration.

# Entreprise ABC

ABC est une entreprise de génie logiciel à forte croissance dont le siège social se trouve au Cap, en Afrique du sud. En tant que prestataire (outsourcer) au service de partenaires multinationaux, ABC met en place des équipes de projets multi-sites ainsi que l'infrastructure associée pour mener à bien, en toute transparence, une vaste gamme de projets de génie logiciel. La croissance actuelle d'ABC est de 30 à 40 % par an. On pense que ce rythme va diminuer pour revenir à 15 à 20 % dans les cinq ans à venir.

## Environnement

Cette section décrit l'environnement matériel et logiciel actuel d'ABC ainsi que la manière dont est mise en œuvre la stratégie de stockage des données.

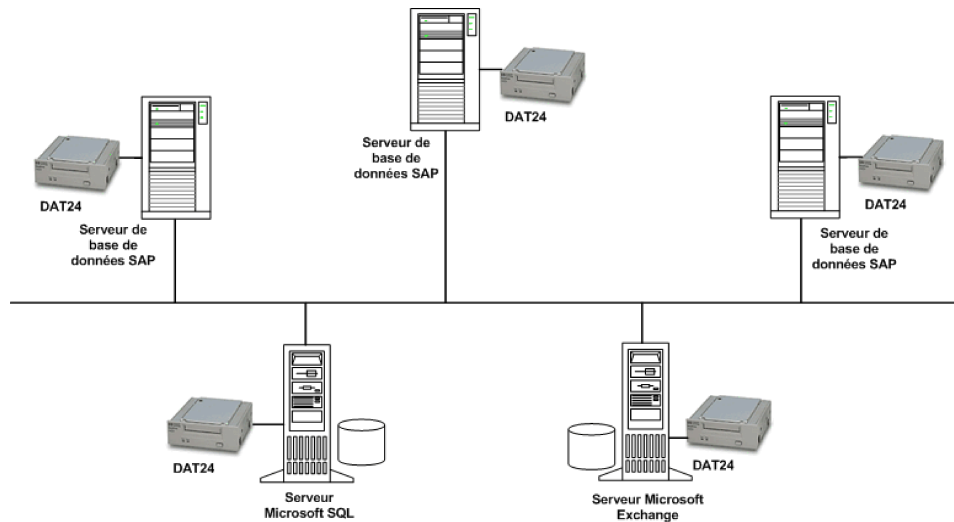
ABC possède des bureaux en trois lieux. Les principales données matérielles relatives à ces trois bureaux sont affichées dans le [Tableau 19](#) à la page 335.

**Tableau 19** Taille de l'environnement de sauvegarde

Lieu	Nb de serveurs Win	Nb de clients Win	Nb de serveurs UX	Nb de clients UX	Qté de données actuelle	Qté de données dans 5 ans	Périphériques actuels
ABC Le Cap	7	55	11	40	100	250	5 DAT24*
ABC Pretoria	5	39	5	32	22	55	1 DAT24*
ABC Durban	3	21	6	59	16	40	1 DAT24*
* chargeur automatique HP StorageWorks DAT24							

Trois services d'ABC Le Cap utilisent la base de données Microsoft SQL pour stocker leurs données, et l'entreprise utilise Microsoft Exchange Server pour ses services de messagerie. Ces bases de données, qui contiennent actuellement respectivement 11 Go et 15 Go de données, sont sauvegardées sur deux chargeurs automatiques HP StorageWorks DAT24.

L'architecture système d'ABC Le Cap comprend notamment le système SAP R/3 avec des bases de données Oracle. Trois serveurs HP T600 sont utilisés comme serveurs de base de données SAP. ABC Le Cap utilise des serveurs d'applications K260 SAP configurés en groupes d'applications : Vente et distribution, Finances et Production. Ces serveurs d'applications ne présentent pas une grande disponibilité. L'environnement de sauvegarde actuel d'ABC Le Cap est décrit dans la [Figure 88](#) à la page 336.



**Figure 88 Topologie de sauvegarde actuelle d'ABC Le Cap**

Actuellement, à ABC Le Cap, les serveurs de base de données SAP sont sauvegardés avec les utilitaires SAP BRBACKUP et SAP BRARCHIVE vers trois chargeurs automatiques HP StorageWorks DAT24. Chaque jour, les données sont copiées manuellement par les employés vers leurs serveurs respectifs. L'administrateur sauvegarde séparément le serveur Microsoft Exchange et la base de données Microsoft SQL vers deux chargeurs automatiques HP StorageWorks DAT24.

Le même système est utilisé dans les bureaux de Durban et de Pretoria, à la différence près que ces succursales ne possèdent pas de système SAP. Les employés copient leurs données vers leurs serveurs respectifs. Chaque jour, les données sont sauvegardées vers un chargeur automatique HP StorageWorks DAT24.

Deux des serveurs d'ABC Pretoria contiennent plus de 500 000 fichiers chacun.

Les supports de sauvegarde sont marqués du nom du service, du nom du serveur et des dates de première et dernière sauvegardes qui y ont été effectuées. A la fin de chaque trimestre, les supports sont envoyés à un établissement central hors site pour y être stockés.



## Problèmes rencontrés avec la solution actuelle

La solution de sauvegarde actuelle présente les inconvénients suivants :

- Il n'y a pas de solution de sauvegarde en ligne pour le serveur de base de données SAP.
- La solution de sauvegarde n'est pas centralisée.
- Les opérations de sauvegarde ne sont pas complètement automatisées.
- La gestion des supports requiert une intervention considérable du personnel.
- La récupération après sinistre est complexe.
- La durée des opérations de sauvegarde est plus longue que la durée autorisée.
- La solution de sauvegarde n'est pas adaptée au rythme de croissance élevé d'ABC.
- Il n'y a aucune génération de rapports ni notification sur les événements importants se rapportant à la sauvegarde.

## Besoins relatifs à une stratégie de sauvegarde

Avant d'aborder les besoins relatifs à la stratégie de sauvegarde d'ABC, vous devez tenir compte des éléments énumérés à la section "[Éléments à prendre en considération](#)" à la page 317.

### Besoins

La section suivante décrit les besoins relatifs à la stratégie de sauvegarde d'ABC.

- Stratégie de l'entreprise en matière de sauvegarde et de restauration :  
Selon la stratégie de l'entreprise pour l'archivage et le stockage de données, des sauvegardes hebdomadaires doivent être effectuées en **12 heures** et des sauvegardes incrémentales quotidiennes doivent être effectuées en **8 heures**.
- Temps d'indisponibilité maximum pour la récupération :  
Le temps d'indisponibilité autorisé a une incidence importante sur le choix des investissements en termes d'infrastructure réseau et de matériel dédié à la sauvegarde. Le tableau suivant donne, pour chaque type de données, le temps d'indisponibilité maximum acceptable pour la récupération des données, c'est-à-

dire le temps pendant lequel des données spécifiques peuvent être indisponibles avant d'être récupérées à partir d'une sauvegarde.

**Tableau 20 Temps d'indisponibilité maximum pour la récupération**

Type de données	Temps d'indisponibilité maximum
Données commerciales de l'entreprise	6 heures
Données de ressources de l'entreprise	6 heures
Données de projet	1 jour
Données personnelles	2 jours

Le temps de récupération correspond essentiellement au temps nécessaire pour accéder aux supports et pour procéder à la restauration des données vers un disque.

- Pendant combien de temps conserver les différents types de données ?

Le [Tableau 21](#) à la page 338 donne la durée de conservation nécessaire pour les différentes données. Cette durée a des répercussions sur le nombre de supports de sauvegarde requis.

**Tableau 21 Durée de conservation nécessaire des données**

Type de données	Durée maximum de stockage des données
Données commerciales de l'entreprise	5 ans
Données de ressources de l'entreprise	5 ans
Données de projet	5 ans
Données personnelles	3 mois

- Comment conserver et gérer les supports contenant des données sauvegardées ?  
Les supports doivent être conservés dans la bibliothèque de bandes de la salle informatique. Toutes les données se trouvant sur le système de sauvegarde de l'entreprise doivent être archivées une fois par semaine par sauvegarde complète et tous les jours par sauvegarde incrémentale. Elles doivent être stockées dans les locaux d'une entreprise de sécurité.

- Quantité de données à sauvegarder :

La quantité actuelle de données à sauvegarder est indiquée dans le [Tableau 22](#) à la page 339 :

**Tableau 22** Quantité de données à sauvegarder

Lieu	Données (en Go)
ABC Le Cap	100
ABC Pretoria	22
ABC Durban	16

Planification en vue de l'augmentation de la quantité de données

ABC prévoit que sa croissance annuelle sera de 15 à 20 %. La quantité de données à sauvegarder devrait donc évoluer en conséquence. Cette évolution aura des répercussions non seulement sur la durée des sauvegardes et sur les périphériques nécessaires à leur réalisation, mais également sur la taille de la base de données IDB.

**Tableau 23** Quantité de données à sauvegarder dans cinq ans

Lieu	Données (en Go)
ABC Le Cap	250
ABC Pretoria	55
ABC Durban	40

- A quelle fréquence sauvegarder les données ?

Une sauvegarde complète de chaque type de données est effectuée une fois par semaine le vendredi, le samedi ou le dimanche. Des sauvegardes incrémentales de niveau un sont effectuées tous les jours ouvrables. Cependant, si une sauvegarde complète est effectuée le vendredi, les sauvegardes incrémentales de niveau un correspondantes sont effectuées les jours ouvrables et le samedi, mais pas le vendredi.

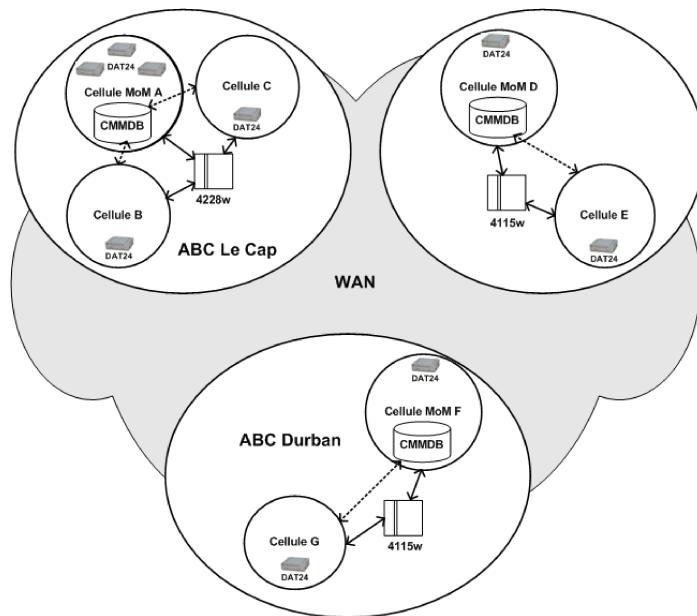
## Solution proposée

Compte tenu des défauts de la solution de sauvegarde actuelle, décrits à la section [Problèmes rencontrés avec la solution actuelle](#) à la page 337, ABC projette de revoir la conception de son système de stockage de données.

### Présentation générale de la solution

Chacun des trois services d'ABC Le Cap doit être configuré dans une cellule Manager-of-Managers (MoM). ABC Durban et ABC Pretoria doivent en outre être configurés en cellules MoM, comportant chacune deux cellules Data Protector.

Configurez la cellule A comme cellule MoM pour l'environnement d'ABC Le Cap, la cellule D comme cellule MoM pour celui d'ABC Pretoria et la cellule F comme cellule MoM pour celui d'ABC Durban. Cette configuration est représentée par la [Figure 89](#) à la page 340.



**Figure 89 Environnement d'entreprise d'ABC**

Les systèmes Gestionnaire de cellule et les Gestionnaires MoM des 7 cellules doivent être des systèmes Windows. Utilisez la base de données centralisée de gestion des supports (CMMDB) dans l'une des cellules de chaque environnement MoM, et des bases de données catalogues dans chacune des 7 cellules. La base de données

centralisée de gestion des supports vous permet de partager des bibliothèques entre des cellules au sein de chaque environnement MoM.

Chacun des trois bureaux d'ABC doit disposer de sa propre bibliothèque. Utilisez la bibliothèque HP StorageWorks DLT 4228w pour l'environnement d'ABC Le Cap, et des bibliothèques HP StorageWorks DLT 4115w pour les environnements d'ABC Pretoria et ABC Durban.

Les trois cellules de l'environnement MoM d'ABC Le Cap doivent disposer chacune d'un serveur de base de données SAP. Ces serveurs se partagent la bibliothèque HP StorageWorks DLT 4228w. Les bases de données Microsoft SQL et Microsoft Exchange sont sauvegardées en local vers des chargeurs automatiques HP StorageWorks DAT24.

Les deux cellules de l'environnement MoM d'ABC Pretoria doivent également se partager une base de données centralisée de gestion des supports. Cette dernière doit être configurée sur le Gestionnaire MoM de la cellule D pour permettre le partage de la bibliothèque HP StorageWorks DLT 4115w entre les cellules.

Les deux cellules de l'environnement MoM d'ABC Durban doivent également se partager une base de données centralisée de gestion des supports. Cette dernière doit être configurée sur le Gestionnaire MoM de la cellule F pour permettre le partage de la bibliothèque HP StorageWorks DLT 4115w entre les cellules.

La solution proposée est décrite en détail ci-dessous :

### Description détaillée de la solution proposée

- Configuration de la cellule :  
Configurez les services en 7 cellules : 3 pour ABC Le Cap, 2 pour ABC Pretoria et 2 pour ABC Durban.

### Pourquoi une configuration en 7 cellules ?

- Les services d'ABC étant séparés géographiquement, il serait difficile de les gérer à partir d'une seule cellule. De plus, il y aurait un risque de problèmes réseau entre les systèmes. La configuration coïncide également avec le nombre de services, ce qui constitue un élément important en terme de sécurité. La taille de chaque cellule correspond également à celle recommandée de 30 à 50 systèmes client. Notez cependant que ce nombre dépend, entre autres, du nombre de fichiers et répertoires présents sur les différents systèmes client.

Configurez ensuite l'environnement de chacun des trois bureaux comme environnement Manager-of-Managers. Ce dernier permet à l'utilisateur de gérer efficacement et en parfaite intégration plusieurs cellules à partir d'un point unique (gestion centralisée). Ceci permet ensuite de configurer la base de données centralisée de gestion des supports (CMMDB) dans chaque environnement MoM.

## Pourquoi utiliser la CMMDB ?

- La base de données centralisée de gestion des supports (CMMDB) permet le partage de périphériques et de supports entre toutes les cellules d'un environnement MoM. Chacun des trois environnements MoM d'ABC peut ainsi utiliser une bibliothèque unique, partagée par les systèmes client de toutes les cellules de l'environnement. L'utilisation d'une seule bibliothèque pour l'ensemble des données d'ABC ne serait guère pertinente, car cela nécessiterait pour la sauvegarde le transfert de grandes quantités de données via un WAN.

Utilisez une base de données catalogue dans chacune des 7 cellules. Les systèmes des cellules peuvent être ceux décrits dans le [Tableau 24](#) à la page 342 :

**Tableau 24 Configuration des cellules d'ABC**

Environnement MoM	Cellule	Nb de serveurs Windows	Nb de clients Windows	Nb de serveurs UNIX	Nb de clients UNIX	Nb de SAP
ABC Le Cap	A*	3	24	2	7	1
	B	2	11	5	21	1
	C	2	20	4	12	1
ABC Pretoria	D*	4	33			
	E	1	6	5	32	
ABC Durban	F*	2	10	4	30	
	p	1	11	2	29	
Le nombre de SAP est le nombre de serveurs de base de données SAP.						
* correspond à une cellule MoM.						

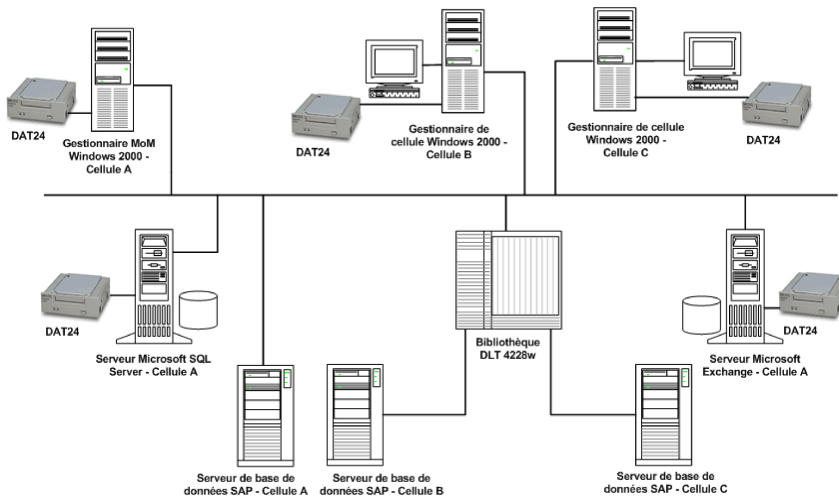
Les systèmes Gestionnaire de cellule et les Gestionnaires MoM des 7 cellules doivent être des systèmes Windows.

## Pourquoi choisir le système Windows ?

- Les systèmes Windows assurent la prise en charge de l'unicode natif et requièrent par conséquent une configuration moins poussée pour le traitement des caractères internationaux dans les noms de fichiers.

Configurez la cellule A en tant que cellule Manager-of-Managers de l'environnement d'ABC Le Cap, et importez le reste des cellules dans l'environnement MoM. Configurez une base de données centralisée de gestion des supports dans la cellule MoM A pour que la même bibliothèque puisse être partagée avec les cellules B et C. Partagez la bibliothèque HP StorageWorks DLT 4228w pour l'environnement d'ABC Le Cap. Avec une capacité de 1,1 To au format compressé, cette bibliothèque devrait suffire pour les besoins prévus de l'entreprise au cours des cinq années à venir.

Les trois cellules d'ABC Le Cap doivent être chacune dotées d'un serveur de base de données SAP. Ces serveurs se partagent la bibliothèque HP StorageWorks DLT 4228w. Les bases de données Microsoft SQL et Microsoft Exchange sont sauvegardées en local vers des chargeurs automatiques HP StorageWorks DAT24. Chacune des cellules de l'environnement doit disposer de sa propre base de données catalogue. Vous trouverez une illustration de la configuration de l'environnement ABC Le Cap dans la [Figure 90](#) à la page 343.



**Figure 90 Environnement de sauvegarde d'entreprise d'ABC Le Cap**

Les deux cellules de l'environnement MoM d'ABC Pretoria doivent se partager une base de données centralisée de gestion des supports. Cette dernière doit être configurée sur le Gestionnaire MoM de la cellule D, afin de permettre le partage de la bibliothèque HP StorageWorks DLT 4115w entre les cellules.

Chacune des cellules de l'environnement doit disposer de sa propre base de données catalogue.

Les deux cellules de l'environnement MoM d'ABC Durban doivent également se partager une base de données centralisée de gestion des supports. Cette dernière doit être configurée sur le Gestionnaire MoM de la cellule F, et chacune des cellules de l'environnement doit avoir sa propre base de données catalogue.

Utilisez une bibliothèque HP StorageWorks DLT 4115w pour l'environnement d'ABC Pretoria et celui d'ABC Durban. Avec une capacité de 600 Go au format compressé, cette bibliothèque devrait suffire pour les besoins de l'entreprise relatifs à chacun de ces environnements prévus pour les cinq années à venir.

### Estimation de la taille de la base de données IDB

L'outil de planification de capacité de la base de données interne a été utilisé pour estimer la taille atteinte en une année par la base de données IDB de la cellule F. Cet outil se trouve à l'emplacement suivant :

- Sur les systèmes Gestionnaire de cellule HP-UX et Solari : `/opt/omni/doc/C/IDB_capacity_planning.xls`
- Sur le système Gestionnaire de cellule Windows : `répertoire_Data_Protector\docs\IDB_capacity_planning.xls`

Les paramètres d'entrée présentés à la [Figure 91](#) à la page 345 comprennent le nombre de fichiers dans l'environnement (2 millions), le facteur de croissance (1,2), la protection des données (260 semaines), la protection de catalogue (3 semaines), le nombre de sauvegardes complètes hebdomadaires (1) et le nombre de sauvegardes incrémentales hebdomadaires (5).



<b>Description de l'environnement</b>	<b>Fichiers :</b>	2	<b>millions</b>
	<b>Fichiers par répertoire :</b>	10	
	<b>Volume de données :</b>	16	<b>Go</b>
	<b>Facteur de croissance :</b>	1,20	
	<b>Performances du périph. :</b>	10,00	<b>Mo/s</b>
	<b>Capacité du support :</b>	70,00	<b>Go</b>
	<b>Objets :</b>	100	
	<b>Modif. par sauv. incrément. :</b>	10,00%	
<b>Paramètres de sauvegarde</b>	<b>Périphériques simult. :</b>	2	
	<b>Taille segment données :</b>	2048,00	<b>Mo</b>
	<b>Niveau de journalisation :</b>	Tout	
	<b>Protection des données :</b>	260	<b>semaines</b>
	<b>Protection du catalogue :</b>	3	<b>semaines</b>
	<b>Sauv. complètes/semaine :</b>	1	
	<b>Sauv. incrémentielles/sem. :</b>	5	
<b>Param. du Gestionnaire de cellule</b>	<b>Vitesse d'insertion :</b>	12	<b>millions/h</b>

**Figure 91 Paramètres d'entrée**

Les résultats sont présentés à la [Figure 92](#) à la page 345. En une année, la base de données devrait croître pour atteindre environ 667,47 Mo.

<b>Résultats/calculs</b>	<b>Taille de fichier moy. :</b>	7,29	<b>Ko</b>	
	<b>Fichiers/segment :</b>	269057,37		
	<b>Taille de catalogue :</b>	16,42	<b>Mo</b>	
	<b>Périphériques K :</b>	2		
	<b>Performances K :</b>	85,48173913	<b>Go/h</b>	
	<b>Durée K :</b>	0,19	<b>heure</b>	
	<b>Supports protégés :</b>	133,7142857		
<b>Estimation espace</b>	<b>MMDB :</b>	30,00	<b>Mo</b>	
	<b>CDB :</b>	<b>Fnames :</b>	207,00	<b>Mo</b>
		<b>Overs :</b>	57,13	<b>Mo</b>
		<b>Mpos :</b>	0,74	<b>Mo</b>
	<b>DCBF :</b>	372,60	<b>Mo</b>	
	<b>SMBF :</b>	5,72	<b>Mo</b>	
	<b>Total :</b>	667,47	<b>Mo</b>	

**Figure 92 Résultats**

Vous pouvez également utiliser l'outil de planification de capacité de la base de données interne pour estimer la taille de la base de données IDB dans les environnements comportant des bases de données en ligne (Oracle, SAP R/3).

- Matériel
  - Réseau

Pour des performances optimales, l'ensemble des systèmes d'un même bureau d'ABC doit se trouver sur le même réseau local. Utilisez le réseau 100TX pour connecter tous les systèmes de chaque bureau, et le WAN pour connecter les cellules des trois bureaux d'ABC. Le réseau 100TX présente un taux de transfert de données de 10 Mo/s, ou 36 Go/h.

- Périphériques de sauvegarde

Les périphériques de sauvegarde sont les suivants: une bibliothèque HP StorageWorks DLT 4228w pour ABC Le Cap et deux bibliothèques HP StorageWorks DLT 4115w pour ABC Pretoria et ABC Durban, ainsi que sept chargeurs automatiques HP StorageWorks DAT24 pour la sauvegarde des fichiers de configuration et de la base de données IDB dans toutes les cellules, et deux chargeurs automatiques HP StorageWorks DAT24 pour la sauvegarde des bases de données Microsoft SQL et Microsoft Exchange à ABC Le Cap. Actuellement, les serveurs Microsoft Exchange et Microsoft SQL hébergent respectivement 15 Go et 11 Go de données, tandis que le reste des données (100 Go - 15 Go - 11 Go = 74 Go) est sauvegardé à l'aide des serveurs de base de données SAP.

### Pourquoi utiliser la bibliothèque HP StorageWorks DLT 4228w ?

- La bibliothèque HP StorageWorks DLT 4228w est dotée de deux lecteurs DLT4000 avec 28 emplacements. Elle présente une capacité totale de stockage compressé de 1,1 To, et un taux de transfert maximum de 6 Mo/s (2 x 3 Mo/s), soit 21 Go/h, avec compression de données. Il s'agit du taux sur lequel nous nous baserons pour la suite de cette section. Actuellement, la quantité totale de données à sauvegarder vers la bibliothèque HP StorageWorks DLT 4228w dans le cadre d'une sauvegarde complète, qu'il s'agisse d'une seule sauvegarde ou d'une planification répartie, est d'environ 74 Go. En supposant que la taille d'une sauvegarde incrémentale corresponde à environ 5 % de celle d'une sauvegarde complète, une génération de sauvegarde, c'est-à-dire une sauvegarde complète plus toutes les sauvegardes incrémentales qui en découlent, nécessite un espace de (74 x 5 % x 5) Go, soit **92,5 Go** dans la bibliothèque. D'ici cinq ans, cet espace nécessaire devrait augmenter pour atteindre environ 230 Go. La stratégie de sauvegarde d'ABC nécessite la conservation de trois générations de sauvegarde de données. Un espace de 230 x 3 Go, soit 690 Go, est donc nécessaire dans la bibliothèque pour le stockage. La capacité de stockage (1,1 To) de la bibliothèque HP StorageWorks DLT 4228w est donc suffisante.

Au Cap, la bibliothèque est partagée entre les trois cellules. A Pretoria, elle est partagée entre les cellules D et E, et à Durban entre les cellules F et G. Ce type de configuration requiert l'utilisation de la base de données centralisée

de gestion des supports Data Protector dans chacun des trois environnements MoM. Ces bases de données sont configurées sur le Gestionnaire MoM des cellules A, D et F.

### Pourquoi utiliser la bibliothèque HP StorageWorks DLT 4115w ?

- La bibliothèque HP StorageWorks DLT 4115w est dotée d'un seul lecteur DLT4000 avec 15 emplacements. Elle présente une capacité totale de stockage compressé de 600 Go et un taux de transfert maximum de 3 Mo/s, ou 10,5 Go/h, avec compression de données. Il s'agit du taux sur lequel nous nous baserons pour la suite de cette section. Actuellement, la quantité totale de données à sauvegarder à Pretoria vers la bibliothèque HP StorageWorks DLT 4115w dans le cadre d'une sauvegarde complète, qu'il s'agisse d'une seule sauvegarde ou d'une planification répartie, est d'environ 22 Go. En supposant que la taille d'une sauvegarde incrémentale corresponde à environ 5 % de celle d'une sauvegarde complète, une génération de sauvegarde, c'est-à-dire une sauvegarde complète plus toutes les sauvegardes incrémentales qui en découlent, nécessite un espace de  $(22 + 22 \times 5 \% \times 5)$  Go, soit **27,5 Go**, dans la bibliothèque. D'ici cinq ans, cet espace nécessaire devrait augmenter pour atteindre environ 68,75 Go. La stratégie de sauvegarde d'ABC nécessite la conservation de trois générations de sauvegarde de données. Un espace de  $68,75 \times 3$  Go, soit 206,25 Go, est donc nécessaire dans la bibliothèque pour le stockage. La capacité de stockage (600 Go) de la bibliothèque HP StorageWorks DLT 4115w est donc suffisante.

Au Cap, des chargeurs automatiques HP StorageWorks DAT24 sont utilisés pour sauvegarder les serveurs Microsoft Exchange et Microsoft SQL ainsi que chacun des sept systèmes Gestionnaire de cellule des trois environnements MoM.

### Pourquoi utiliser le chargeur automatique HP StorageWorks DAT24 ?

- Le chargeur automatique HP StorageWorks DAT24 est doté de six cartouches de données de 24 Go. Elle présente une capacité totale de stockage compressé de 144 Go et un taux de transfert maximum de 2 Mo/s, ou 7 Go/h, avec compression de données. Il s'agit du taux sur lequel nous nous baserons pour la suite de cette section. Actuellement, la quantité totale de données à sauvegarder au Cap vers le chargeur automatique HP StorageWorks DAT24 (connecté au serveur Microsoft Exchange mentionné plus haut) est de 15 Go. En supposant que la taille d'une sauvegarde incrémentale corresponde à environ 5 % de celle d'une sauvegarde complète, une génération de sauvegarde, c'est-à-dire une sauvegarde complète plus toutes les sauvegardes incrémentales qui en

découlent, nécessite un espace de  $(15 + 15 * 5 \% * 5)$  Go, soit **18,75 Go**. D'ici cinq ans, cet espace nécessaire devrait augmenter pour atteindre environ 47 Go. La stratégie de sauvegarde d'ABC nécessite la conservation de deux générations de sauvegarde de données. Un espace de  $47 * 2$  Go, soit **94 Go**, est donc nécessaire dans la bibliothèque pour le stockage. La capacité de stockage (144 Go) du chargeur automatique HP StorageWorks DAT24 est donc suffisante.

### Combien de temps dure une sauvegarde complète ?

Au Cap, les serveurs de base de données SAP des trois cellules contiennent environ 7 Go de données à sauvegarder vers une bibliothèque HP StorageWorks DLT 4228w. Cette dernière est dotée de deux lecteurs et présente un taux de transfert de données de 6 Mo/s ( $2 * 3$  Mo/s), ou 21 Go/h. La sauvegarde des données dure par conséquent **5 heures maximum**. La quantité de données prévue dans cinq ans, soit 185 Go, devrait être sauvegardée en **9 à 10 heures**, ce qui reste inférieur aux 12 heures autorisées.

Les cellules D et E d'ABC Pretoria partagent une bibliothèque HP StorageWorks DLT 4115w. Cette dernière est dotée d'un seul lecteur et présente un taux de transfert de données de 3 Mo/s ou 10,5 Go/h. La quantité totale de données à sauvegarder dans ces cellules est d'environ 22 Go. La sauvegarde devrait donc prendre entre **2 et 3 heures**. La quantité de données prévue dans cinq ans, soit 55 Go, devrait être sauvegardée en **5 à 7 heures**, ce qui reste inférieur aux 12 heures autorisées.

De même, les 16 Go de données présents dans les cellules F et G d'ABC Durban doivent pouvoir être sauvegardés en **2 heures maximum**. La quantité de données prévue dans cinq ans, soit 40 Go, devrait être sauvegardée en **4 heures environ**, ce qui reste inférieur aux 12 heures autorisées.

La plus grande base de données catalogue Data Protector (1,3 Go) d'ABC Pretoria peut être sauvegardée en quelques minutes si aucune vérification d'intégrité n'est effectuée au préalable. Par défaut, Data Protector vérifie l'intégrité de la base de données avant que celle-ci ne soit sauvegardée. Cette vérification prend moins d'une heure pour une base de données de 1,3 Go. Par conséquent, les fichiers de configuration et la base de données IDB d'ABC Pretoria doivent pouvoir être sauvegardés en moins de **2 heures**.

- Pools de supports

Les supports sont regroupés dans des pools pour être mieux suivis et contrôlés. Les pools de supports facilitent la gestion d'un grand nombre de supports, réduisant ainsi au minimum les efforts de gestion des administrateurs. Utilisez la

structure de l'organisation et les critères des catégories de systèmes pour définir les pools de supports suivants :

**Tableau 25 Utilisation des pools de supports d'ABC**

Nom du pool de supports	Lieu	Description
CT_SAP_Pool	Le Cap	Serveur de base de données SAP
CT_SQL_Pool	Le Cap	Microsoft SQL Server
CT_Exchange_Pool	Le Cap	Microsoft Exchange Server
CT_DB_Pool	Le Cap	IDB
P_DLT_Pool	Pretoria	Bibliothèque HP StorageWorks DLT 4115w
P_DAT_Pool	Pretoria	Chargeurs automatiques HP StorageWorks DAT24
P_DB_Pool	Pretoria	IDB (base de données interne)
D_DLT_Pool	Durban	Bibliothèque HP StorageWorks DLT 4115w
D_DAT_Pool	Durban	Chargeurs automatiques HP StorageWorks DAT24
D_DB_Pool	Durban	IDB (base de données interne)

- Spécifications de sauvegarde

Configurez les spécifications de sauvegarde comme suit :

- DB\_A...G :

Spécifications de sauvegarde pour chacune des 7 bases de données IDB et les fichiers de configuration. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète par semaine et une sauvegarde incrémentale de niveau un tous les jours à 03:00, sauf le dimanche.

## Pourquoi utiliser les sauvegardes différentielles (Incr. 1) ?

- Pour restaurer les données les plus récentes, seuls deux jeux de supports sont nécessaires, l'un pour la dernière sauvegarde complète et l'autre pour la dernière sauvegarde incrémentale de niveau 1 précédant la restauration. Cela permet de simplifier et d'accélérer considérablement le processus de restauration. Lorsque des sauvegardes incrémentales simples sont effectuées, le nombre de jeux de supports peut augmenter considérablement, rendant le processus de restauration plus complexe et plus lent.

Pour des raisons de sécurité, il est recommandé d'effectuer deux copies des fichiers de configuration et de la base de données IDB.

- SAP\_A...C :

Spécification de sauvegarde pour les serveurs de base de données SAP respectivement dans les cellules A, B et C. Utilisez la planification répartie pour éviter une surcharge du réseau ou des périphériques ainsi que les problèmes de fenêtre temporelle décrits dans le [Tableau 26](#) à la page 350 :

**Tableau 26 Planification répartie pour ABC Le Cap**

	Lun	Mar	Mer	Jeu	Ven	Sam	Dim
Cellule A	Incr. 1	Incr. 1	Incr. 1	Incr. 1	Complète	Incr. 1	
Cellule B	Incr. 1	Incr. 1	Incr. 1	Incr. 1	Incr. 1	Complète	
Cellule C	Incr. 1	Incr. 1	Incr. 1	Incr. 1	Incr. 1		Complète

- SERVERS\_A...G :

Spécifications de sauvegarde des serveurs de l'entreprise pour la préparation à une récupération après sinistre. Cette spécification de sauvegarde est mise à jour à chaque installation d'un nouveau serveur ou mise à niveau d'un serveur existant. Planifiez les spécifications de sauvegarde de sorte que Data Protector exécute des sauvegardes complètes comme indiqué au [Tableau 27](#) à la page 351 et des sauvegardes incrémentales de niveau un tous les jours ouvrables.

- USERS\_D...G :

Spécifications de sauvegarde pour les données utilisateur. Il s'agit de la sauvegarde de production principale à ABC Pretoria et ABC Durban. Planifiez

la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète hebdomadaire chaque vendredi comme indiqué au [Tableau 27](#) à la page 351 et des sauvegardes incrémentales de niveau un tous les jours ouvrables. Cependant, si une sauvegarde complète est effectuée le vendredi, les sauvegardes incrémentales de niveau un correspondantes sont effectuées les jours ouvrables et le samedi, mais pas le vendredi.

La configuration de la spécification de sauvegarde est expliquée plus en détails dans le [Tableau 27](#) à la page 351.

**Tableau 27 Configuration de spécification de sauvegarde pour ABC**

Nom	Cellule	Description	Jour de sauvegarde	Heure
DB_A	A	IDB	Samedi	03:00
DB_B	B	IDB	Samedi	03:00
DB_C	C	IDB	Samedi	03:00
SQL_A	A	Base de données Microsoft SQL	Vendredi	20:00
EXCHANGE_A	A	Base de données Microsoft Exchange	Vendredi	20:00
SAP_A	A	Serveur de base de données SAP	Vendredi	20:00
SAP_B	B	Serveur de base de données SAP	Samedi	20:00
SAP_C	C	Serveur de base de données SAP	Dimanche	20:00
SERVERS_A	A	Serveurs	Vendredi	23:00
SERVERS_B	B	Serveurs	Samedi	23:00
SERVERS_C	C	Serveurs	Dimanche	23:00
DB_D	D	IDB	Samedi	03:00
DB_E	E	IDB	Samedi	03:00
SERVERS_D	D	Serveurs	Vendredi	23:00

Nom	Cellule	Description	Jour de sauvegarde	Heure
SERVERS_E	E	Serveurs	Samedi	23:00
USERS_D	D	Données utilisateur	Samedi	0:00
USERS_E	E	Données utilisateur	Dimanche	0:00
DB_F	F	IDB	Samedi	03:00
DB_G	G	IDB	Samedi	03:00
SERVERS_F	F	IDB	Vendredi	23:00
SERVERS_G	G	Serveurs	Samedi	23:00
USERS_F	F	Données utilisateur	Samedi	0:00
USERS_G	G	Données utilisateur	Dimanche	0:00

## Options de sauvegarde

Utilisez les options de sauvegarde Data Protector par défaut. Définissez les options comme suit :

- Journaliser répertoires

Cette option de sauvegarde de système de fichiers permet de s'assurer que seules les informations des répertoires sont stockées dans la base de données catalogue. La fonction de recherche est désactivée pendant la restauration et vous ne pouvez parcourir que les répertoires. Utilisez cette option pour sauvegarder les deux serveurs de la cellule D contenant plus de 500 000 fichiers chacun. Sinon, la taille de la base de données catalogue Data Protector risque d'augmenter considérablement.

- Protection

Les données doivent pouvoir être accessibles pendant trois semaines. Une sauvegarde complète devant avoir lieu chaque semaine, choisissez une protection de catalogue de 27 jours (3 semaines x 7 jours + 6 jours = 27 jours).

Choisissez une protection de données de 5 ans pour toutes les spécifications de sauvegarde, sauf Exchange\_A qui sert à la sauvegarde du courrier personnel. Pour cette spécification de sauvegarde, optez pour une protection de données de 3 mois.



- **Simultanéité**  
Réglez sur 5 le nombre d'Agents de disque pouvant écrire simultanément des données dans la bibliothèque. Vous améliorerez ainsi les performances de sauvegarde.
- **Pool de supports**  
Sélectionnez les pools de supports et les supports appropriés pour la sauvegarde.
- **Génération de rapports et notifications**  
Des notifications envoyées par e-mail aux administrateurs de sauvegarde sont définies pour les demandes de montage, en cas d'espace insuffisant dans la base de données, en cas d'erreur de périphérique et à la fin des sessions pour toutes les spécifications de sauvegarde. Eventuellement, des notifications par e-mail ou message de diffusion sont définies pour les utilisateurs finaux souhaitant être informés de la réussite des sauvegardes de leurs systèmes.  
Pour permettre à tous les utilisateurs de connaître facilement l'état de leurs sauvegardes, définissez comme suit les informations de sauvegarde client sur la page d'accueil de l'entreprise :
  1. Configurez un groupe de rapports avec un rapport sur la sauvegarde client pour chaque client. Le rapport doit être enregistré dans le fichier au format HTML.
  2. Planifiez le groupe de rapports.
  3. Reliez les fichiers contenant les rapports à la page d'accueil de l'entreprise.
- **Mise au coffre**  
La mise au coffre consiste à stocker des supports en lieu sûr pendant une période déterminée.  
Des supports sont déplacés une fois par semaine vers le coffre, et remplacés par de nouveaux supports dans les bibliothèques HP StorageWorks DLT 4228w et 4115w, et les chargeurs automatiques HP StorageWorks DAT24. Toutes les actions, hormis le déplacement de supports vers le coffre, sont exécutées par la solution logicielle, notamment les requêtes effectuées en interne dans la base de données pour éviter à l'administrateur d'avoir à rechercher les supports devant être éjectés.  
Effectuez le suivi des supports déplacés vers un coffre. Cette opération est utile lorsque vous souhaitez restaurer des données à partir de sauvegardes réalisées sur un support déplacé vers le coffre. Data Protector vous permet d'effectuer les tâches de mise au coffre suivantes :
  - Génération de rapports sur les supports stockés à un endroit spécifique et dont la protection des données expire à une date déterminée

- Génération de rapports sur les supports utilisés pour une sauvegarde au cours d'une période donnée
- Affichage d'une liste de spécifications de sauvegarde ayant utilisé des supports spécifiques lors de la sauvegarde
- Affichage d'une liste de supports nécessaires pour les opérations de restauration et des emplacements physiques où sont stockés ces supports
- Filtrage des supports à partir de l'affichage des supports selon des critères spécifiques (affichage des supports dont la protection a expiré, par exemple)
- Restauration
  - Restaurer par requête
 

Les demandes de restauration par requête sont envoyées à l'administrateur. Si la dernière sauvegarde des fichiers date de moins de 3 semaines avant l'envoi de la requête, l'administrateur peut utiliser l'option Restaurer par requête pour sélectionner les fichiers et répertoires à restaurer selon des critères déterminés. Il choisit ensuite l'option Ecraser pour remplacer les fichiers et répertoires du disque par les versions figurant sur le support.
  - Restauration complète de système de fichiers
 

Les demandes de restauration de systèmes de fichiers entiers sont envoyées à l'administrateur. Si la dernière sauvegarde des fichiers date de moins de 3 semaines avant l'envoi de la demande, l'administrateur peut sélectionner l'objet à restaurer et utiliser l'option Restaurer dans.

Les objets sont alors restaurés avec la même structure de répertoires dans un répertoire sélectionné. Servez-vous d'un utilitaire Windows ou UNIX pour comparer les objets restaurés aux objets sauvegardés.
  - Restauration à partir d'un coffre
 

Pour restaurer des données à partir d'un coffre, sauvegardées par exemple 3 ans auparavant, envoyez une demande à l'administrateur, qui effectue alors les opérations suivantes :

    1. Il identifie les supports nécessaires à la restauration.
    2. Il déplace les supports du coffre vers la bibliothèque HP StorageWorks DLT 4228w, la bibliothèque HP StorageWorks DLT 4115w ou vers un autre périphérique, puis les analyse.
    3. Si les supports ne se trouvent pas dans la base de données catalogue Data Protector, il sélectionne l'objet spécifique à restaurer à l'aide de l'option Lister depuis supports.
    4. Il effectue la restauration.

---

# B Informations complémentaires

## Dans cette annexe

La présente annexe fournit des informations supplémentaires sur certains aspects des concepts de Data Protector, notamment les générations de sauvegarde, des exemples de copie automatisée des supports et l'internationalisation.

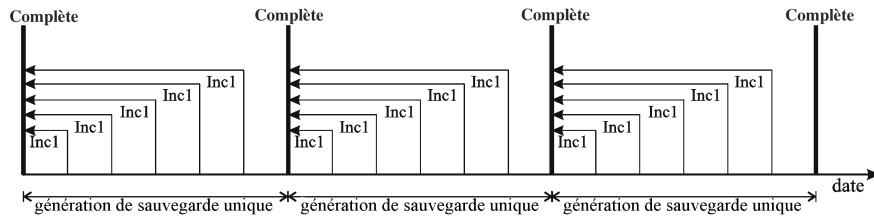
## Génération de sauvegarde

Data Protector propose un modèle de protection associé à l'heure/la date. Il est facile d'établir une correspondance entre un modèle de sauvegarde basé sur les générations et le modèle basé sur l'heure, à condition que les sauvegardes soient effectuées régulièrement.

### Qu'est-ce qu'une génération de sauvegarde ?

Une génération de sauvegarde (voir [Figure 93](#) à la page 356) est constituée d'une sauvegarde complète ainsi que de toutes les sauvegardes incrémentales basées sur cette sauvegarde complète. Lorsque la sauvegarde complète suivante est effectuée, une nouvelle génération de sauvegarde est créée.

Les générations de sauvegarde permettent de savoir combien de versions complètes de données sauvegardées ont été réalisées. Pour pouvoir effectuer une restauration de l'état à un instant donné, vous devez disposer d'au moins une génération de sauvegarde (c'est-à-dire une sauvegarde complète ainsi que toutes les incrémentales jusqu'à cet instant). Conservez plusieurs générations de sauvegarde (trois par exemple), selon la stratégie de protection des données adoptée par votre entreprise.



**Figure 93 Générations de sauvegarde**

Pour configurer Data Protector afin qu'il conserve automatiquement le nombre souhaité de générations de sauvegarde, choisissez les durées de protection des données et de catalogue adéquates et planifiez les sauvegardes sans surveillance (complètes et incrémentales).

Pour conserver par exemple trois générations de sauvegarde alors que vous effectuez une sauvegarde complète par semaine et une sauvegarde incrémentale remise à niveau par jour, définissez la protection des données à  $7 \times 3 + 6 = 27$  jours. Une génération de sauvegarde est constituée d'une sauvegarde complète ainsi que de toutes les sauvegardes incrémentales effectuées jusqu'à la prochaine sauvegarde complète : par conséquent, le chiffre six dans la formule représente les sauvegardes incrémentales effectuées avant la génération de sauvegarde suivante (soit la quatrième) et appartenant à la troisième génération de sauvegarde.

Vous pouvez établir une rotation automatique des supports (pour les supports dont le temps de protection a expiré) avec une politique d'utilisation des pools appropriée. Pour plus de détails, reportez-vous à la section "[Mise en œuvre d'une stratégie de rotation des supports](#)" à la page 158.

## Exemples de copie automatisée des supports

A la fin d'une sauvegarde, vous pouvez faire appel à la fonctionnalité de copie automatisée pour dupliquer les supports de sauvegarde, puis transférer les originaux ou les copies dans un coffre hors site. Selon la disponibilité des périphériques, vous pouvez opter pour la copie post-sauvegarde ou la copie planifiée.

Les aspects suivants sont à prendre en compte :

- Il est conseillé d'effectuer toutes les sauvegardes dans un premier temps puis de copier les supports.
- Durant la copie, les supports en cours de duplication ne sont pas disponibles pour la restauration.
- Vous pouvez uniquement copier un support en intégralité et non des objets spécifiques.

- Après la copie, les supports originaux et leurs copies deviennent des supports sans possibilité d'ajout : vous ne pouvez plus ajouter de sauvegarde sur ces supports.
- Pour la copie de supports planifiée, les périphériques et supports requis doivent impérativement être disponibles à la date/l'heure planifiée : toute indisponibilité entraîne l'abandon de l'opération.

## Exemple 1 : copie automatisée des supports de sauvegarde de systèmes de fichiers

Votre entreprise dispose d'un environnement MoM doté de deux cellules contenant chacune 150 systèmes informatiques (serveurs et stations de travail). Chaque système dispose en moyenne de 10 Go de données, soit au total 3000 Go à sauvegarder.

Vous souhaitez effectuer des sauvegardes quotidiennes Incr1, des sauvegardes hebdomadaires complètes et des sauvegardes mensuelles complètes à des fins d'archivage. Les sauvegardes doivent être effectuées en dehors des heures ouvrées de l'entreprise, ce qui signifie qu'elles peuvent débuter après 17h00 et doivent s'achever avant 8h00 le lendemain matin ; elles peuvent également être effectuées en fin de semaine.

Vous décidez de créer des copies des supports de sauvegarde, que vous conserverez sur site pour les besoins de restauration, et de transférer les supports originaux dans un coffre hors site pour des raisons de sécurité. La copie doit avoir lieu après les sauvegardes. Pour cela, vous allez utiliser la copie automatisée de supports (AMC - Automated Media Copying).

Vous utilisez une bibliothèque de bandes HP StorageWorks 6/60 dotée de 6 lecteurs LTO et des supports LTO Ultrium 1. Par expérience, vous savez que le taux de transfert des données est d'environ 80 Go par heure et que la capacité moyenne d'un support est de 153 Go.

Après l'opération de copie des supports, les supports source et cible sont sans possibilité d'ajout. De ce fait, il est préférable de limiter le nombre de supports requis pour la sauvegarde. Il est conseillé d'utiliser pour commencer des supports vides et d'exploiter leur capacité maximale. A cette fin, vous pouvez créer des spécifications de sauvegarde avec un seul périphérique affecté. De cette façon, un nouveau support n'est utilisé que lorsque le support en cours d'utilisation est plein. Toutefois, cela augmente la durée de la sauvegarde par rapport à l'écriture simultanée sur plusieurs supports.

Vous décidez de créer 4 spécifications de sauvegarde. Pour économiser l'espace sur les supports, les données sont divisées entre les spécifications de sauvegarde de manière à utiliser le nombre minimum possible de supports. Chaque sauvegarde se déroule sur un seul périphérique.

La copie automatisée des supports est effectuée à la fin de la sauvegarde. Vous pouvez utiliser tous les périphériques disponibles pour l'opération. Cela signifie que 3 périphériques seront respectivement utilisés pour les supports sources et pour les supports cibles.

La durée estimée de la copie sera approximativement égale à celle de la sauvegarde.

## Sauvegarde Incr1

### Configuration des sauvegardes

Vous planifiez des sauvegardes Incr1 chaque jour du lundi au jeudi à 18:00. La protection des données est définie sur 4 semaines. En supposant que 30 % des données sont modifiées chaque jour, cela représente 900 Go de données à sauvegarder. Les données sont divisées entre les spécifications de sauvegarde de la manière suivante :

- SpécSauveg1 (lecteur 1) - 300 Go
- SpécSauveg2 (lecteur 2) - 300 Go
- SpécSauveg3 (lecteur 3) - 150 Go
- SpécSauveg4 (lecteur 4) - 150 Go

Les spécifications de sauvegarde 1 et 2 requièrent deux supports chacune et la sauvegarde dure environ 4 heures. Les spécifications de sauvegarde 3 et 4 requièrent un support chacune et la sauvegarde dure environ 2 heures.

### Configuration de la copie automatisée des supports

La copie automatisée des supports de chaque sauvegarde commence une fois la sauvegarde terminée. Vous avez 6 supports à copier et pouvez utiliser tous les lecteurs de la bibliothèque pour l'opération, dès qu'ils deviennent disponibles.

Pour copier les supports résultant des spécifications 1 et 2, vous pouvez utiliser la copie de supports post-sauvegarde ; deux lecteurs (lecteur 5 et lecteur 6) étant libres, vous n'avez pas à vous soucier de la disponibilité des périphériques.

Configurez la copie de supports post-sauvegarde pour la spécification 1 et sélectionnez le lecteur 1 comme périphérique source, puis le lecteur 6 comme périphérique cible. Vous définissez la même protection des données que pour l'original et spécifiez l'emplacement des supports (par exemple, Etagère 1).

Configurez également la copie de supports post-sauvegarde pour la spécification 2 et sélectionnez le lecteur 2 comme périphérique source, puis le lecteur 5 comme périphérique cible. Vous définissez la même protection des données que pour l'original et spécifiez l'emplacement des supports.

Pour copier les supports résultant des spécifications de sauvegarde 3 et 4, optez pour la copie planifiée : en effet, vous allez utiliser les lecteurs 3 et 4 pour la copie et devrez attendre que chacune des deux sauvegardes se termine. Notez que si les périphériques ne sont pas disponibles au moment où la copie des supports est programmée, l'opération échouera. C'est la raison pour laquelle il est recommandé d'ajouter une certaine marge à la durée estimée de la sauvegarde lors de la programmation de l'opération de copie automatisée des supports qui utilisera les mêmes périphériques.

Planifiez l'opération de copie une heure après la fin prévue de la sauvegarde, sélectionnez les supports résultant des spécifications 3 et 4 comme supports à copier, puis choisissez le lecteur 3 comme périphérique source et le 4 comme cible. Vous définissez la même protection des données que pour l'original et spécifiez l'emplacement des supports.

Pour obtenir une représentation graphique de la sauvegarde Incr1 et de la copie automatisée des supports, reportez-vous à la [Figure 94](#) à la page 360.

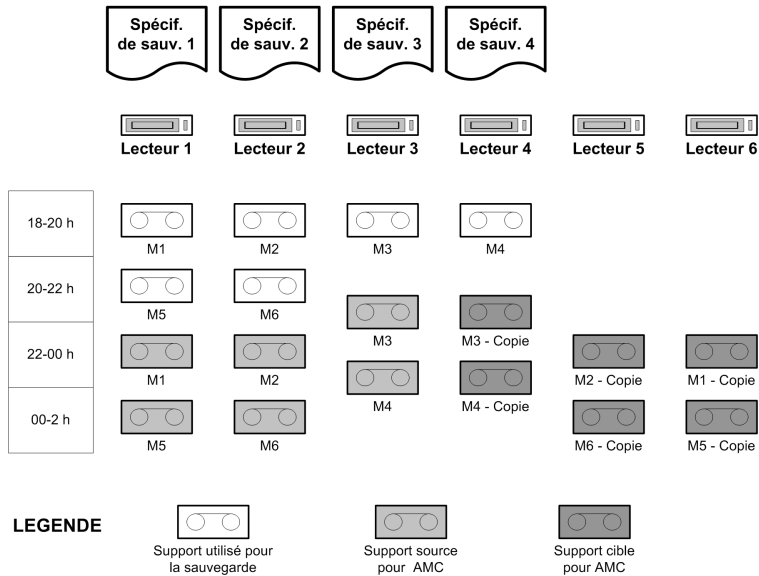


Figure 94 Sauvegarde Incr1 et copie automatisée de supports

## Sauvegarde complète

### Configuration des sauvegardes

Vous programmez la sauvegarde hebdomadaire complète pour le vendredi à 18:00. La protection des données est définie sur 8 semaines. Vous avez 3000 Go de données à sauvegarder. Les données sont divisées entre les spécifications de sauvegarde de la manière suivante :

- SpécSauveg1 (lecteur 1) - 1000 Go
- SpécSauveg2 (lecteur 2) - 1000 Go
- SpécSauveg3 (lecteur 3) - 500 Go
- SpécSauveg4 (lecteur 4) - 500 Go

Les spécifications de sauvegarde 1 et 2 requièrent chacune 7 supports, tandis que les spécifications 3 et 4 en nécessitent 4 chacune. La sauvegarde s'effectue en 14 heures environ.



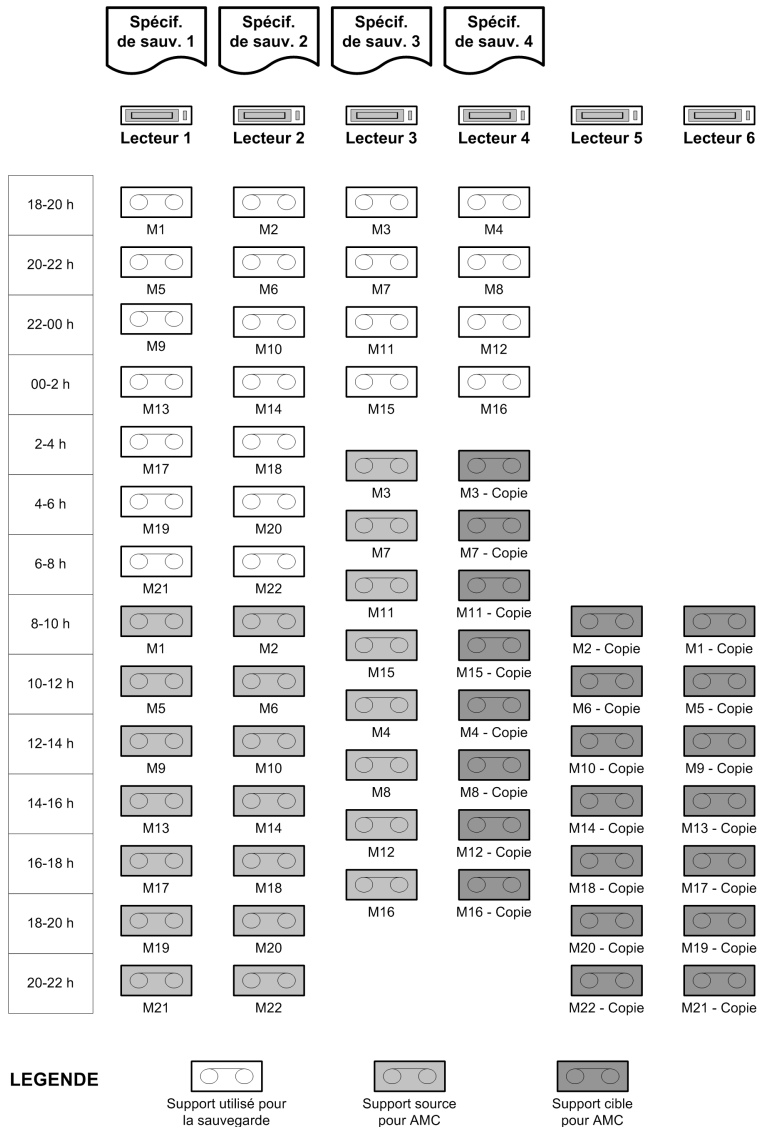
## Configuration de la copie automatisée des supports

La copie automatisée des supports de chaque sauvegarde commence une fois la sauvegarde terminée. Vous avez 22 supports à copier et tous les périphériques sont utilisés dès qu'ils sont disponibles.

Encore une fois, vous utilisez la copie de supports après sauvegarde pour copier les supports utilisés avec SpécSauveg1 et SpécSauveg2, et la copie programmée pour les supports utilisés pour SpécSauveg3 et SpécSauveg4.

Les périphériques et les paramètres de protection des données sont identiques à ceux qui ont été utilisés pour la copie de la sauvegarde Incr1. La copie programmée des supports commence une heure après l'heure de fin estimée de la sauvegarde.

Pour obtenir une représentation graphique de la sauvegarde complète et de la copie automatisée des supports, reportez-vous à la [Figure 95](#) à la page 362.

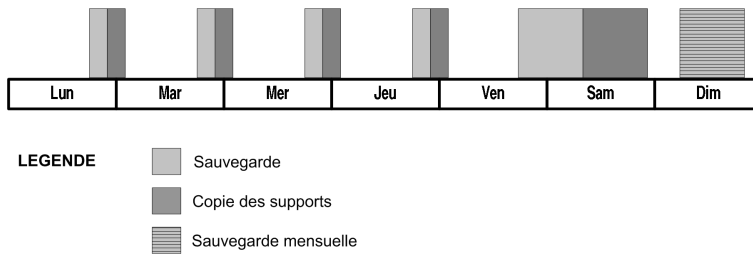


**Figure 95 Sauvegarde complète et copie automatisée de supports**

Vous programmez votre sauvegarde mensuelle complète pour le dimanche à 6:00. Cette sauvegarde étant destinée à l'archivage, elle n'est pas habituellement copiée.

La [Figure 96](#) à la page 363 présente un aperçu général des périodes d'occupation des périphériques. Notez qu'il s'agit d'une présentation grossière, de sorte que le

graphique ne tient pas compte du chevauchement partiel de certaines sessions de sauvegarde et de copie.



**Figure 96 Présentation des sessions de sauvegarde et de copie automatisée des supports**

## Exemple 2 : copie automatisée des supports de sauvegardes de base de données Oracle

Votre entreprise dispose d'une base de données Oracle de 500 Go. Vous souhaitez effectuer quotidiennement une sauvegarde complète de la base de données. La sauvegarde doit être effectuée en dehors des heures ouvrées de l'entreprise, ce qui signifie qu'elle peut débuter après 17h00 et doit s'achever avant 8h00 le lendemain matin ; elle peut également être effectuée en fin de semaine.

Vous utilisez la copie automatisée pour copier les supports de sauvegarde ; ces copies resteront sur le site à des fins de restauration. Les originaux seront déplacés vers un coffre hors site par mesure de sécurité. Les supports doivent être copiés après la fin de la sauvegarde. Pour ce faire, vous utiliserez la copie des supports après sauvegarde.

Vous utilisez une bibliothèque de bandes HP StorageWorks 10/700 dotée de 10 lecteurs LTO et des supports LTO Ultrium 1. En fonction de votre expérience passée, vous estimez que le transfert des données s'effectue au rythme d'environ 80 Go par heure ; la capacité moyenne d'un support est de 153 Go.

Après l'opération de copie des supports, les supports utilisés pour la sauvegarde et la copie des supports sont sans possibilité d'ajout ; par conséquent, il peut être préférable d'utiliser autant d'espace que possible sur la bande. Par ailleurs, vous souhaitez que la sauvegarde se termine dès que possible. Vous utilisez 4 périphériques pour la sauvegarde. Il est recommandé de commencer avec des supports vierges et d'utiliser pleinement leur capacité.

La copie automatisée des supports commence après la fin de la sauvegarde. Vous avez 4 supports à copier et affectez par conséquent 8 périphériques à cette opération.

Cela signifie que 4 périphériques seront respectivement utilisés pour les supports source et pour les supports cible.

On estime que la durée de la copie des supports sera environ équivalente à la durée de la sauvegarde.

## Sauvegarde complète

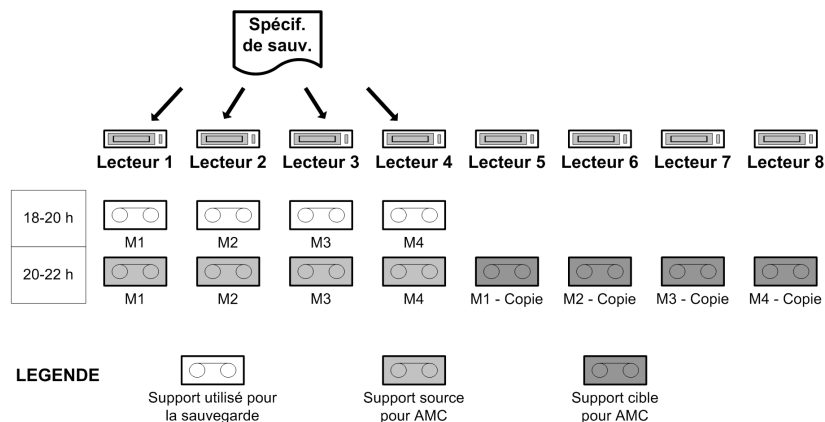
### Configuration des sauvegardes

Vous programmez la sauvegarde complète quotidienne chaque jour du lundi au vendredi à 18:00. La protection des données est définie sur 4 semaines. Vous avez 500 Go de données à sauvegarder. Vous utilisez les lecteurs 1, 2, 3 et 4. La sauvegarde utilise 4 supports et s'effectue en 2 heures environ.

### Configuration de la copie automatisée des supports

Vous utilisez la copie des supports après sauvegarde car vous disposez d'un nombre suffisant de périphériques. Vous spécifiez les lecteurs 1, 2, 3 et 4 en tant que périphériques sources et les lecteurs 5, 6, 7 et 8 en tant que périphériques cibles. Vous définissez la même protection des données que pour l'original et spécifiez l'emplacement des supports.

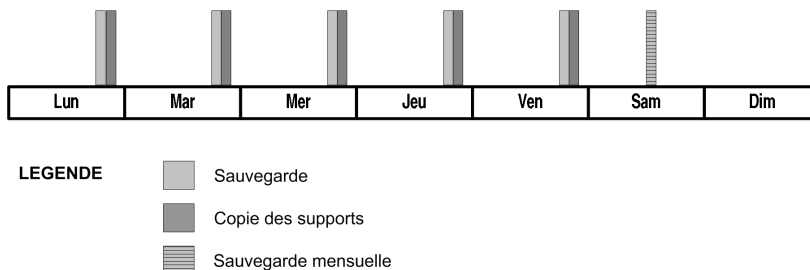
Pour obtenir une représentation graphique de la sauvegarde complète de la base de données et de la copie automatisée des supports, reportez-vous à la [Figure 97](#) à la page 364.



**Figure 97 Sauvegarde complète de base de données et copie automatisée de supports**

Vous programmez votre sauvegarde complète mensuelle pour le samedi à midi. Cette sauvegarde étant destinée à l'archivage, elle n'est pas habituellement copiée.

La Figure 98 à la page 365 présente un aperçu général des périodes d'occupation des périphériques.



**Figure 98** Présentation des sessions de sauvegarde et de copie automatisée des supports

## Internationalisation

L'internationalisation consiste à développer et à mettre en œuvre un logiciel de sorte que le produit interagisse avec la langue maternelle de l'utilisateur, et conformément aux paramètres locaux de l'utilisateur (devise, heure, date, nombres et autres formats). L'utilisateur peut ainsi saisir les données de texte dans sa langue et les afficher correctement. L'internationalisation, dans le cadre du développement d'un logiciel, est la procédure qui permet de mettre en œuvre un logiciel avec un code source et un code binaire uniques. Ce sont les textes proprement dits (indépendants des binaires) qui sont traduits afin de localiser le logiciel en plusieurs langues. L'internationalisation est donc un processus destiné à permettre la localisation. Data Protector est un produit internationalisé dont l'interface utilisateur est proposée en plusieurs langues.

## Localisation

La localisation consiste à adapter un produit ou un service à une langue et à une culture particulières. Il s'agit notamment de proposer des écrans, une aide en ligne, des messages d'erreurs, des manuels et autres éléments localisés.

Au lieu d'envoyer les chaînes de message proprement dites, Data Protector envoie les ID des chaînes provenant des agents au Gestionnaire de cellule. Ensuite, le Gestionnaire de cellule transfère les chaînes à l'interface, laquelle affiche les messages dans le format de langue approprié. Notez que les noms des répertoires et des fichiers ne sont pas indexés. Ils sont transmis sous forme de chaînes de texte et présentés tels quels dans l'interface. Les implications de cette démarche sont traitées dans la section "[Gestion des noms de fichier](#)" à la page 366.

Data Protector est localisé en plusieurs langues. Pour plus d'informations sur les langues disponibles, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector* ou adressez-vous à votre fournisseur ou à votre service de vente HP.

## Gestion des noms de fichier

La gestion des noms de fichier dans un environnement hétérogène (différents systèmes d'exploitation et différents paramètres locaux dans une même cellule) est un défi important. Data Protector traite les noms selon les différents paramètres locaux (tels que la langue, la zone géographique et les jeux de caractères) utilisés sur le système lors de la création des noms de fichier. Les noms de fichier qui ont été sauvegardés à l'aide de certains paramètres locaux puis affichés ou restaurés à l'aide d'autres paramètres locaux, requièrent une configuration spécifique pour s'afficher correctement.

## Quelques explications

Les différents fournisseurs de plates-formes utilisent une grande diversité de représentations de caractères ou de normes d'encodage des caractères (telles qu'ISO 8859-1, Shift-JIS, EUC, Code Page 932 et Unicode) pour prendre en charge les différents jeux de langues. Ces codages entrent en conflit les uns avec les autres - deux codages peuvent utiliser la même valeur pour deux caractères *différents* ou bien différentes valeurs pour le *même* caractère. Après la création d'un nom de fichier, aucun jeu de codes ayant été utilisé n'est indiqué. Il se peut que les noms de fichier transmis entre plusieurs systèmes au moyen de différents codages ne s'affichent pas dans l'interface graphique.

La transmission de données entre différentes plates-formes n'est pas problématique si toutes les plates-formes utilisent une implémentation d'Unicode (UTF-16 sous Windows et UTF-xx sur d'autres plates-formes) acceptant tous les caractères.

Malheureusement, l'implémentation UTF-xx d'Unicode n'est pas une norme sur les systèmes UNIX. Les composants de l'application peuvent être répartis sur plusieurs systèmes et plates-formes, tels que Windows, HP-UX, Solaris et AIX. Les données résidant sur ces différentes plates-formes doivent être sauvegardées et restaurées. A défaut de pouvoir compenser l'absence d'une représentation commune à l'échelle du secteur pour les langues et les jeux de caractères, Data Protector atténue son impact pour l'utilisateur.

## Exemple

Avec certaines configurations dans des environnements hétérogènes, les noms de fichier peuvent apparaître altérés dans l'interface graphique. Lors de l'utilisation de Data Protector, il est possible par exemple de sauvegarder des fichiers sur une plate-forme HP-UX sur laquelle l'Agent de disque est en cours d'exécution, et d'afficher ces fichiers dans l'interface graphique Data Protector qui fonctionne sous Windows. A moins que des jeux de codes identiques ne soient utilisés sur les deux plates-formes, il se peut que les noms de fichier ne s'affichent pas correctement. Cela est dû au fait que la même valeur de caractère peut avoir une signification et une apparence différentes selon le jeu de codes utilisé.

## Exemple d'incompatibilité avec UNIX

Trois utilisateurs travaillant sous un système Solaris sur lequel Data Protector n'est pas installé et utilisant des jeux de caractères différents créent des fichiers sous le même système de fichiers, hors plage de caractères ASCII. Si les utilisateurs se servent alors de la commande `ls` pour afficher les fichiers qu'ils ont créés ainsi que ceux créés par les autres utilisateurs, la situation suivante apparaît :

- Chaque utilisateur voit ses propres noms de fichier correctement affichés.
- Chaque utilisateur voit les noms de fichier des autres utilisateurs comme altérés. Les noms de fichier altérés peuvent apparaître différemment sous les divers systèmes.

Les noms de fichier altérés ont été créés avec un jeu de codes différent de celui utilisé pour exécuter la commande `ls`. Ils ne sont pas dotés d'une balise indiquant le jeu de codes utilisé pour leur création. Ce phénomène se produit sur les systèmes utilisant des afficheurs de systèmes de fichiers natifs, par exemple `ls` dans la fenêtre du terminal.

## Gestion des noms de fichier lors d'une sauvegarde

Data Protector lit les noms de fichier à l'aide de l'Agent de disque (lequel s'exécute sur le client à sauvegarder) et enregistre une copie originale sur un support. Si l'option `log filename` est activée pour la sauvegarde, les noms de fichier sont également convertis dans un jeu de codes "interne" et reliés à la base de données interne.

## Exploration des noms de fichier

Il est possible de sélectionner les fichiers via l'interface Data Protector avant la restauration. Pour cela, il suffit d'afficher les noms de fichier dans la base de données IDB sur le système exécutant l'interface graphique. Data Protector propose plusieurs codages pour visualiser les noms de fichier apparaissant dans son interface

graphique. Lorsqu'un codage de caractères spécifique est utilisé, Data Protector l'utilise pour afficher les caractères dans les noms de fichier.

Pour afficher correctement des noms de fichier, sélectionnez le codage de caractères utilisé sur le système sur lequel les fichiers ont été créés. Dans le cas contraire, les noms de fichier apparaissent altérés dans l'interface graphique de Data Protector.

Les noms de fichier altérés peuvent être restaurés sur la plate-forme sur laquelle les sauvegardes ont été effectuées.

Pour obtenir la liste des configurations indiquant les restrictions en matière d'exploration des noms de fichier, recherchez l'entrée suivante dans l'index de l'aide en ligne : "internationalisation".

## Gestion des noms de fichier lors d'une restauration

Les fichiers sont généralement restaurés sur la plate-forme utilisée pour les sauvegardes. La procédure se déroule comme suit :

- Vous devez sélectionner les fichiers à restaurer dans l'interface.
- Data Protector recherche sur la bande les données correspondantes et les restaure.
- Les noms de fichier originaux (c'est-à-dire les copies originales provenant de la bande) sont restaurés.



---

# Glossaire

<b>ACSL</b>	<i>(terme propre à StorageTek)</i> Automated Cartridge System Library Server (ACSL), serveur de bibliothèque à système de cartouche automatisé - logiciel chargé de la gestion du système de cartouche automatisé (ACS).
<b>Active Directory</b>	<i>(terme propre à Windows)</i> 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.
<b>affichage de sauvegarde</b>	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.
<b>agent d'application</b>	Composant requis sur un client pour sauvegarder ou restaurer les intégrations de bases de données en ligne. <i>Voir aussi <a href="#">Agent de disque</a>.</i>
<b>Agent de disque</b>	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. Au cours d'une session de vérification d'objet, l'Agent de disque reçoit des données de l'Agent de support et exécute le processus de vérification, mais aucune donnée n'est écrite sur le disque.

- Agent de support** 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. Lors d'une session de restauration ou de vérification d'objet, un Agent de support localise les données stockées sur le support de sauvegarde et les envoie à l'Agent de disque en vue de leur traitement. Lors d'une session de restauration, l'Agent de disque écrit les données sur le disque. Un Agent de support gère également le contrôle robotique d'une bibliothèque.
- Agent EMC Symmetrix** Module logiciel Data Protector qui prépare l'environnement EMC Symmetrix aux opérations de sauvegarde et de restauration.
- Agent HP StorageWorks P6000 EVA SMI-S** Module logiciel de Data Protector qui exécute toutes les tâches nécessaires à l'intégration HP StorageWorks P6000 EVA Disk Array Family. Avec l'Agent P6000 EVA SMI-S, le contrôle sur la baie est assuré par le fournisseur HP StorageWorks SMI-S P6000 EVA Array qui dirige la communication entre les demandes entrantes et HP StorageWorks CV EVA. [Voir aussi HP StorageWorks Command View \(CV\) EVA](#) et [fournisseur HP StorageWorks SMI-S P6000 EVA Array](#).
- Agent HP StorageWorks P9000 XP** Composant logiciel de Data Protector qui exécute toutes les tâches nécessaires à l'intégration de Data Protector avec HP StorageWorks P9000 XP Disk Array Family. Il communique avec le système de stockage P9000 XP Array à l'aide de l'utilitaire Gestionnaire RAID P9000 XP (sur les systèmes HP-UX et Windows) ou de la bibliothèque du Gestionnaire RAID (sur les systèmes Solaris).
- Agent SSE (SSEA)** *(terme propre à HP)* Voir [HP StorageWorks Agent P9000 XP](#).

**P9000 XP Array  
Family)**

<b>Agents de disque simultanés</b>	Nombre d'Agents de disque autorisés à envoyer des données simultanément à un Agent de support.
<b>AML</b>	<i>(terme propre à ADIC/GRAU)</i> Automated Mixed-Media library, bibliothèque de supports mixtes automatisée.
<b>AMU</b>	<i>(terme propre à ADIC/GRAU)</i> Archive Management Unit, unité de gestion d'archive.
<b>analyse</b>	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.
<b>API C Lotus</b>	<i>(terme propre à Lotus Domino Server)</i> Interface destinée à l'échange de données de sauvegarde et de récupération entre Lotus Domino Server et une solution de sauvegarde comme Data Protector.
<b>API de sauvegarde</b>	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.
<b>API de serveur de sauvegarde Sybase</b>	<i>(terme propre à Sybase)</i> Interface standard développée pour l'échange de données de sauvegarde et de récupération entre un serveur Sybase SQL et une solution de sauvegarde telle que Data Protector.
<b>application compatible cluster</b>	Application prenant en charge l'API cluster (Application Programming Interface). Chaque application compatible cluster déclare ses propres ressources stratégiques (volumes de disques (sous Microsoft Cluster Server), groupes de volumes (sous

MC/ServiceGuard), services d'application, noms et adresses IP, etc.).

- archivage des journaux** *(terme propre à Lotus Domino Server)* Mode de connexion à la base de données Lotus Domino Server qui permet de n'écraser les fichiers journaux de transactions qu'après leur sauvegarde.
- auto-migration** *(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](#).
- BACKINT** *(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.
- bande virtuelle** *(terme propre à VLS)* Technologie d'archivage qui sauvegarde les données sur des lecteurs de disque de la même manière 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](#).
- banque d'informations** *(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](#).
- banque de boîtes aux lettres** *(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.

<b>banque de clés</b>	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).
<b>banque de dossiers publics</b>	<i>(terme propre à Microsoft Exchange Server)</i> 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.
<b>basculement</b>	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.
<b>basculement</b>	<i>(terme propre à HP P6000 EVA Array Family)</i> Opération qui renverse les rôles entre source et destination dans les configurations HP Continuous Access + Business Copy (CA + BC) P6000 EVA. <a href="#">Voir aussi HP Continuous Access + Business Copy (CA + BC) P6000 EVA.</a>
<b>Base de données centralisée de gestion des supports (CMMDB)</b>	Voir <a href="#">CMMDB</a> .
<b>base de données cible</b>	<i>(terme propre à Oracle)</i> Terme utilisé dans le contexte du Gestionnaire de récupération (RMAN). La base de données cible est celle qui est sauvegardée ou restaurée.
<b>Base de données d'enregistrement des classes COM+</b>	<i>(terme propre Windows)</i> La base de données de registres de classe COM+ et la base de registres 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.
<b>base de données du catalogue de récupération</b>	<i>(terme propre à Oracle)</i> Base de données Oracle contenant un schéma de catalogue de récupération. Il est recommandé de

ne pas stocker le catalogue de récupération dans la base de données cible.

<b>Base de données du gestionnaire de supports amovibles</b>	<i>(terme propre à Windows)</i> Service Windows pour la gestion de supports amovibles (tels que des bandes et des disques) et de périphériques de stockage (bibliothèques). Le stockage sur supports amovibles permet aux applications d'accéder aux ressources de mêmes supports et de les partager.
<b>base de données ZDB</b>	<i>(terme propre à la sauvegarde ZDB)</i> Partie de la base de données interne stockant des informations sur la sauvegarde ZDB, telles que les volumes sources, les répliques et les données de sécurité. La base de données ZDB est utilisée pour la sauvegarde avec temps d'indisponibilité nul, la restauration instantanée et la restauration Split Mirror. <i>Voir aussi <a href="#">sauvegarde avec temps d'indisponibilité nul (ZDB)</a>.</i>
<b>bases de données système</b>	<i>(terme propre à Sybase)</i> Les quatre bases de données système d'un Sybase SQL Server nouvellement installé sont les suivantes : <ul style="list-style-type: none"><li>• base de données principale (master)</li><li>• base de données temporaire (tempdb)</li><li>• base de données de procédures système (sybssystemprocs)</li><li>• base de données modèle (model)</li></ul>
<b>BC</b>	<i>(terme propre à EMC Symmetrix)</i> Business Continance - Procédé permettant aux utilisateurs d'accéder et de gérer des copies instantanées des périphériques standard EMC Symmetrix. <i>Voir aussi <a href="#">BCV</a>.</i>
<b>BCV</b>	<i>(terme propre à EMC Symmetrix)</i> Business Continance Volumes ou périphériques BCV - il s'agit de SLD dédiés, préconfigurés dans l'ICDA sur lequel l'opération Business Continance 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. <i>Voir aussi <a href="#">BC</a> et <a href="#">Processus BC</a>.</i>
<b>bibliothèque</b>	Egalement appelée "changeur automatique", "bibliothèque de banques magnéto-optiques", "chargeur automatique" ou "échangeur". Une bibliothèque contient des supports stockés dans des emplacements référentiels. 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.

**bibliothèque de bandes magnéto-optiques**

Voir [bibliothèque](#).

**bibliothèque de bandes virtuelle (VTL)**

*(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 \(VLS\)](#).

**bibliothèque de base de données**

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, le serveur Oracle par exemple.

**bibliothèque du Gestionnaire RAID**

*(terme propre à HP P9000 XP Array Family)* 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 P9000 XP Disk Array Family, ainsi qu'aux fonctions clés de HP StorageWorks P9000 XP Disk Array Family au moyen d'appels de fonction convertis en une séquence de commandes SCSI de bas niveau.

**bibliothèque StorageTek ACS**

*(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.

**boîte aux lettres**

*(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.

**BRARCHIVE**

*(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](#).

- BRBACKUP** *(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](#).
- BRRESTORE** *(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](#).
- BSM** 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.
- canal** *(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 'disk'
  - type 'sbt\_tape'
- Si le canal spécifié est de type 'sbt\_tape' et qu'Oracle est intégré avec Data Protector, le processus du serveur essaie de lire les sauvegardes ou d'écrire les fichiers de données sur Data Protector.
- CAP** *(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.



<b>caractère générique</b>	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.
<b>catalogue de récupération</b>	<p>(<i>terme propre à Oracle</i>) 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 :</p> <ul style="list-style-type: none"> <li>• le schéma physique de la base de données cible Oracle,</li> <li>• les jeux de sauvegarde de fichiers de données et de journaux d'archive,</li> <li>• les copies de fichiers de données,</li> <li>• les journaux de rétablissement archivés,</li> <li>• les scripts stockés.</li> </ul>
<b>CDB</b>	<p>La base de données catalogue est une partie de la base de données IDB qui contient des informations sur les sessions de sauvegarde, de restauration, de copie d'objet, de consolidation d'objet, de vérification d'objet et de gestion de support. 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 <a href="#">MMDB</a>.</p>
<b>cellule</b>	Ensemble de systèmes contrôlés par un Gestionnaire de cellule. Une cellule représente généralement les systèmes d'un site ou d'une entité organisationnelle connectés au même réseau local/SAN. Un contrôle centralisé permet d'administrer les tâches et les stratégies de sauvegarde et de restauration.
<b>Certificate Server</b>	Un Certificate Server (ou serveur de certificats) Windows peut être installé et configuré pour fournir des certificats aux clients. Il propose des services personnalisables d'émission et de gestion de certificats pour l'entreprise. Ces services permettent d'émettre, de résilier et de gérer les certificats utilisés dans les technologies de cryptographie à clé publique.

<b>chaîne de périphériques</b>	Série de périphériques autonomes configurés pour une utilisation séquentielle. Lorsqu'un support est plein dans un périphérique, la sauvegarde se poursuit automatiquement sur un support du périphérique suivant dans la chaîne de périphériques.
<b>chaîne de restauration</b>	Toutes les sauvegardes nécessaires à la restauration d'un objet sauvegarde à un point dans le temps donné (version). Une chaîne de restauration consiste en une sauvegarde complète de l'objet et un certain nombre de sauvegardes incrémentales liées.
<b>chaîne de sauvegarde</b>	Voir <a href="#">chaîne de restauration</a> .
<b>changeur automatique</b>	Voir <a href="#">bibliothèque</a> .
<b>chargeur automatique</b>	Voir <a href="#">bibliothèque</a> .
<b>chargeurs</b>	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.
<b>clé de cryptage</b>	Un numéro 256 bits généré au hasard utilisé par l'algorithme de cryptage Data Protector pour coder des informations pendant les sauvegardes pour lesquelles le cryptage sur logiciel ou sur lecteur 256 bits a été spécifié. La même clé sert au décryptage ultérieur des informations. Les clés de cryptage pour une cellule Data Protector sont stockées dans une banque de clés centrale dans le Gestionnaire de cellule.
<b>clé de session</b>	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 <code>omnimnt</code> , <code>omnistat</code> et <code>omniabort</code> .
<b>client d'interface Java</b>	Le client d'interface Java est un composant de l'interface utilisateur graphique Java qui contient uniquement les

fonctionnalités liées à l'interface utilisateur (interface utilisateur graphique du Gestionnaire de cellule et interface utilisateur graphique du Manager-of-Managers (MoM)) et qui doit être connecté au serveur d'interface Java pour fonctionner.

<b>client de gestion VMware</b>	<p>(<i>terme propre à l'intégration VMware</i>) 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 autonome ESX Server).</p>
<b>client ou système client</b>	<p>Tout système configuré avec des fonctions Data Protector et dans une cellule.</p>
<b>Cluster Continuous Replication</b>	<p>(<i>terme propre à Microsoft Exchange Server</i>) Cluster Continuous Replication (CCR) 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.</p> <p>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 <a href="#">Service de réplication Exchange</a> et <a href="#">Local Continuous Replication</a>.</p>
<b>CMMDB</b>	<p>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 Manager-of-Managers. Une connexion réseau</p>

fiable entre la cellule MoM et les autres cellules Data Protector est vivement recommandée.

Voir aussi [MoM](#).

**Command View  
VLS**

(*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 [système de bibliothèques virtuelles \(VLS\)](#).

**commandes pré- et  
post-exécution**

Les commandes pré- et post-exécution servent à réaliser une action supplémentaire avant et après une session de sauvegarde ou de restauration. Elles 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.

**communications de  
contrôle cryptées**

Data Protector sécurise les échanges entre les clients de la cellule Data Protector, sur la base du protocole SSL (Secure Socket Layer) qui utilise des algorithmes SSLv3 pour crypter les communications de contrôle. Les communications de contrôle dans une cellule Data Protector correspondent à tous les échanges entre les processus Data Protector, à l'exception du transfert de données de l'Agent de disque (et des intégrations) vers l'Agent de support, et vice versa.

**compte utilisateur  
(compte utilisateur  
Data Protector)**

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 de 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.

**consolidation  
d'objet**

Processus permettant de fusionner une chaîne de restauration d'un objet sauvegarde, comprenant une sauvegarde complète et 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.

<b>conteneur</b>	<i>(terme propre à HP P6000 EVA Array Family)</i> Espace sur une baie de disques qui est préalloué pour une utilisation ultérieure en tant que snapshot standard, vsnap ou snapclone.
<b>contrôleur de domaine</b>	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.
<b>copie d'objet</b>	Copie d'une version spécifique d'un objet créé au cours d'une session de copie d'objets ou de sauvegarde avec la fonction de mise en miroir d'objets.
<b>copie intelligente</b>	<i>(terme propre à VLS)</i> Copie des données sauvegardées créée à partir de la bande virtuelle vers 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. <i>Voir aussi <a href="#">système de bibliothèques virtuelles (VLS)</a>.</i>
<b>copie miroir</b>	<i>(terme propre à Microsoft VSS)</i> Volume représentant une copie du volume d'origine à un instant 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. <i>Voir aussi <a href="#">Microsoft Volume Shadow Copy Service</a> et <a href="#">réplique</a>.</i>
<b>création de réplique Split Mirror</b>	<i>(terme propre à EMC Symmetrix et à HP P9000 XP Array Family)</i> Technique de création de réplique selon laquelle un ensemble de volumes cibles pré-configuré (un miroir) est synchronisé en permanence avec un ensemble de volumes sources jusqu'à ce qu'une réplique du contenu des volumes sources soit requise. La synchronisation est alors arrêtée (le miroir est séparé) et une réplique Split Mirror des volumes sources au moment de la séparation est conservée dans les volumes cibles. <i>Voir aussi <a href="#">Split Mirror</a>.</i>
<b>création de snapshot</b>	<i>(terme propre à HP P6000 EVA Array Family, HP P9000 XP Array Family et HP StorageWorks P4000 SAN Solutions)</i> Processus de création de réplique permettant de générer des copies de volumes sources sélectionnés au moyen de technologies de virtualisation du stockage. Une telle réplique est créée à un instant donné et est immédiatement utilisable. Toutefois, avec certains types de snapshot, un processus de

copie des données en arrière-plan continue d'être exécuté sur la baie de disques après la création de la réplique.

Voir aussi [snapshot](#).

<b>CRS</b>	Processus (service) CRS (Cell Request Server ou serveur des requêtes de cellule) qui s'exécute sur le Gestionnaire de cellule 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 <code>root</code> .
<b>cryptage AES 256 bits</b>	Data Protector sur logiciel, 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. La même clé 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.
<b>cryptage sur lecteur</b>	Le cryptage sur lecteur Data Protector utilise la fonctionnalité de cryptage du lecteur. Lors de la sauvegarde, le lecteur crypte les données et les métadonnées qui sont écrites sur le support.
<b>CSM</b>	Le processus CSM Data Protector (Copy and Consolidation Session Manager - gestionnaire de session de copie et de consolidation) contrôle les sessions de copie et de consolidation d'objets et s'exécute sur le système Gestionnaire de cellule.
<b>Dbobject</b>	<i>(terme propre à Informix Server)</i> Objet de base de données physique Informix Server. Il peut s'agir d'un blobspace, d'un dbspace ou d'un fichier journal logique.
<b>DCBF</b>	Les fichiers binaires de catalogue des détails (DCBF, pour Detail Catalog Binary Files), une partie de la base de données interne, contiennent les informations relatives aux attributs et aux versions de fichier. Ils occupent environ 80 % de l'espace de l'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.
<b>délai d'expiration de la protection de données</b>	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](#).

<b>demande de montage</b>	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.
<b>dépôt de fichier</b>	Fichier contenant les données d'une sauvegarde vers un périphérique de bibliothèque de fichiers.
<b>disque auxiliaire</b>	Disque amorçable possédant un système d'exploitation minimum avec réseau et Agent de disque Data Protector installé. Il peut être transporté et utilisé pour amorcer le système cible dans la première phase de la récupération après sinistre avec restitution de disque des clients UNIX.
<b>disque virtuel</b>	<i>(terme propre à HP P6000 EVA Array Family)</i> Unité de stockage allouée à partir d'un pool de stockage d'une baie de disques HP StorageWorks P6000 EVA Disk Array Family. Le disque virtuel est l'entité qui peut être répliquée à l'aide de la fonctionnalité Snapshot de la baie de disques. Voir aussi <a href="#">volume source</a> et <a href="#">volume cible</a> .
<b>disques partagés</b>	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.
<b>DMZ</b>	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.
<b>données sauvegardées publiques/privées</b>	Lors de la configuration d'une sauvegarde, l'utilisateur peut indiquer si les données sauvegardées seront : <ul style="list-style-type: none"><li>• publiques, c'est-à-dire visibles (et accessibles pour la restauration) par tous les utilisateurs de Data Protector</li><li>• privées, c'est-à-dire visibles (et accessibles pour la restauration) uniquement par le propriétaire de la sauvegarde et par les administrateurs.</li></ul>

<b>données_ programme_Data_Protector</b>	Sous Windows Vista, Windows 7 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 <a href="#">répertoire_Data_Protector</a> .
<b>DR OS</b>	Environnement de système d'exploitation dans lequel la récupération après sinistre est effectuée. Il fournit à Data Protector un environnement d'exécution de base (accès au disque, au réseau, à la bande et au système de fichiers). Vous devez installer sur disque ou charger en mémoire et configurer le système d'exploitation avant d'exécuter la récupération après sinistre Data Protector. Le DR OS peut être temporaire ou actif. Un DR OS temporaire est exclusivement utilisé en tant qu'environnement hôte pour la restauration d'un autre système d'exploitation, conjointement avec les données de configuration du système d'exploitation cible. Il est supprimé à l'issue de la restauration du système cible dans la configuration système d'origine. Un DR OS actif héberge le processus de récupération après sinistre Data Protector et peut également faire partie du système restauré, car il remplace ses propres données de configuration par celles d'origine.
<b>droits d'accès</b>	Voir <a href="#">droits utilisateur</a> .
<b>droits utilisateur</b>	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.
<b>échangeur</b>	Egalement appelé échangeur SCSI. Voir aussi <a href="#">bibliothèque</a> .
<b>emplacement</b>	Position mécanique au sein d'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.
<b>emplacement d'un support</b>	Emplacement physique d'un support défini par l'utilisateur, par exemple, "bâtiment 4" ou "stockage hors site".



<b>enregistrement circulaire</b>	<i>(terme propre à Microsoft Exchange Server et Lotus Domino Server)</i> L'enregistrement circulaire est un mode de base de données Microsoft Exchange Server et Lotus 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.
<b>environnement de sauvegarde d'entreprise</b>	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 <a href="#">MoM</a> .
<b>espace de table</b>	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.
<b>établissement (rétablissement) incrémental</b>	<i>(terme propre à EMC Symmetrix)</i> 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.
<b>état de paire</b>	<i>(terme propre à HP P9000 XP Array Family)</i> Etat d'une paire de disques (volume secondaire et volume principal correspondant) d'une baie de disques HP StorageWorks P9000 XP Disk Array Family. L'état des paires de disques varie en fonction des circonstances. Les états suivants sont particulièrement importants pour le fonctionnement de l'Agent HP StorageWorks P9000 XP Data Protector : <ul style="list-style-type: none"> <li>• PAIR – Le volume secondaire est préparé pour la sauvegarde avec temps d'indisponibilité nul. S'il s'agit d'un miroir, il est</li> </ul>

complètement synchronisé et s'il s'agit d'un volume à utiliser pour le stockage des snapshots, il est vide.

- **SUSPENDED** – Le lien entre les disques est suspendu. Toutefois, la relation de paire est maintenue et le disque secondaire peut à nouveau être préparé pour la sauvegarde avec temps d'indisponibilité nul.
- **COPY** – La paire de disques est occupée et en cours de transition vers l'état PAIR. Si le volume secondaire est un miroir, il est resynchronisé avec le volume principal, et s'il s'agit d'un volume à utiliser pour le stockage des snapshots, son contenu est effacé.

<b>état des supports</b>	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.
<b>état système</b>	<i>(terme propre à Windows)</i> 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 du système indiquent, par ailleurs, les points de contrôle du registre des ressources et le journal de récupération de ressource quorum, qui contient les informations à jour sur la base de données des clusters.
<b>étiquette de support</b>	Identificateur défini par l'utilisateur et servant à décrire un support.
<b>exécution multsnap</b>	<i>(terme propre à HP P6000 EVA Array Family)</i> Création simultanée de volumes cibles pour assurer la cohérence des données de sauvegarde sur chacun des volumes cibles, mais aussi sur tous les volumes constituant un snapshot. <i>Voir aussi <a href="#">snapshot</a>.</i>
<b>exportation de supports</b>	Procédé consistant à supprimer de la base de données IDB toutes les données relatives aux sessions de sauvegarde (comme les systèmes, objets et noms des fichiers qui résident sur le

support). 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](#).

<b>facteurs d'état des supports</b>	Limites d'âge et de réécriture définies par l'utilisateur pour déterminer l'état d'un support.
<b>Fibre Channel</b>	Norme ANSI pour l'interconnexion informatique à haute 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.
<b>fichier CDF</b>	<i>(terme propre à UNIX)</i> 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.
<b>fichier d'amorçage d'urgence</b>	<i>(terme propre à Informix Server)</i> Fichier de configuration Informix Server <code>ixbar.server_id</code> qui réside dans le répertoire <code>INFORMIXDIR/etc</code> (sous Windows) ou <code>INFORMIXDIR\etc</code> (sous UNIX). <code>INFORMIXDIR</code> est le répertoire de base d'Informix Server et <code>ID_serveur</code> la valeur du paramètre de configuration <code>SERVERNUM</code> . Chaque ligne du fichier d'amorçage d'urgence correspond à un objet sauvegarde.
<b>fichier d'options globales</b>	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 se trouve sur le Gestionnaire de cellule dans le répertoire <code>données_programme_Data_Protector\Config\Server\Options</code> (Windows Server 2008), <code>répertoire_Data_Protector\Config\Server\Options</code> (autres systèmes Windows) ou /

etc/opt/omni/server/options (systèmes HP-UX, Solaris et Linux).

- fichier de contrôle** *(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.
- fichier de données** *(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.
- fichier de données de récupération système** Voir [fichier DRS](#).
- fichier de récupération de l'IDB** Fichier 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 et les journaux de transactions de l'IDB sur un disque physique séparé des autres répertoires de l'IDB, mais aussi de créer une autre copie du fichier.
- fichier DRS** *(terme propre à la récupération après sinistre)* Fichier texte au format Unicode (UTF-16), généré au cours de la sauvegarde de la CONFIGURATION d'un système Windows ou Linux et stocké sur le Gestionnaire de cellule. Il contient les informations système requises pour installer et configurer le système d'exploitation sur le système cible en cas de sinistre.  
Voir aussi [système cible](#).
- fichier épars** 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, cette opération peut s'avérer impossible.
- fichier Jours chômés** 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 données\_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).

**fichier P1S**

Fichier P1S contenant 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). Créé durant la sauvegarde complète, il est enregistré sur un support de sauvegarde et sur le Gestionnaire de cellule dans le répertoire données\_programme\_Data\_Protector\  
Config\Server\dr\pls (Windows Server 2008),  
répertoire\_Data\_Protector\Config\Server\dr\pls  
(autres systèmes Windows) ou /etc/opt/omni/server/dr/  
pls (systèmes UNIX), sous le nom recovery.pls.

**fichier sqlhosts ou  
registre**

*(terme propre à Informix Server)* Registre (sous Windows) ou fichier d'informations de connectivité Informix Server (sous UNIX) 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.

**fichier sst.conf**

Le fichier /usr/kernel/drv/sst.conf doit être présent sur chaque client Sun 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.

**fichier st.conf**

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.

**fichier  
TSANDS.CFG**

*(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.

**fichier  
user\_restrictions**

Fichier qui restreint certaines opérations, disponibles pour le groupe d'utilisateurs Data Protector en fonction des droits utilisateur affectés, que les utilisateurs peuvent effectuer sur des

systèmes spécifiques de la cellule Data Protector. Ces restrictions s'appliquent uniquement aux groupes d'utilisateurs Data Protector autres que *Administrateur* et *Opérateur*.

<b>fichiers de journal des transactions</b>	Il s'agit des fichiers dans lesquels sont enregistrées les modifications de base de données. Ils assurent également une fonction de tolérance aux pannes en cas de sinistre au niveau d'une base de données.
<b>fichiers de récupération</b>	<i>(terme propre à Oracle)</i> Les fichiers de récupération sont des fichiers propres à Oracle 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. <i>Voir aussi <a href="#">zone de récupération flash</a>.</i>
<b>fichiers journaux logiques</b>	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 d'implémenter toutes les transactions qui ont été transférées et d'annuler toutes celles qui ne l'ont pas encore été.
<b>flux de données</b>	Séquence de données transférées via le canal de communication.
<b>fnames.dat</b>	Les fichiers <code>fnames.dat</code> 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.
<b>format de support de fichiers distribués</b>	Format de support, disponible avec la bibliothèque de fichiers, qui prend en charge un type de sauvegarde synthétique très économe en espace disque, appelée "sauvegarde complète virtuelle". L'utilisation de ce format est une condition préalable à la sauvegarde complète virtuelle. <i>Voir aussi <a href="#">sauvegarde complète virtuelle</a>.</i>
<b>formatage</b>	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.

<b>fournisseur de copie miroir</b>	<p>(<i>terme propre à Microsoft VSS</i>) Entité réalisant la création et la représentation des copies miroir des volumes. Les fournisseurs possèdent les données des copies miroir et exposent les copies miroir. Ces fournisseurs peuvent être de type logiciel (fournisseurs système, par exemple) ou matériel (disques locaux, baies de disques).</p> <p>Voir aussi <a href="#">copie miroir</a>.</p>
<b>fusion</b>	<p>La fusion correspond à un mode de résolution de conflit 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.</p> <p>Voir aussi <a href="#">réécriture</a>.</p>
<b>Fournisseur HP StorageWorks SMI-S P6000 EVA Array</b>	<p>Interface permettant de contrôler HP StorageWorks P6000 EVA Disk Array Family. Le fournisseur SMI-S P6000 EVA Array s'exécute en tant que service distinct sur le système de gestion du stockage HP et agit comme passerelle entre les requêtes entrantes et HP StorageWorks Command View EVA. Grâce à l'intégration de Data Protector avec HP P6000 EVA Array Family, le fournisseur SMI-S P6000 EVA Array accepte les requêtes standardisées de l'Agent P6000 EVA SMI-S, communique avec HP StorageWorks Command View EVA pour l'appel d'informations ou de méthodes et renvoie des réponses standardisées.</p> <p>Voir aussi <a href="#">HP StorageWorks Agent P6000 EVA SMI-S</a> et <a href="#">HP StorageWorks Command View (CV) EVA</a>.</p>
<b>génération de rapports Web</b>	<p>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.</p>
<b>génération de sauvegarde</b>	<p>Une génération de sauvegarde est constituée d'une sauvegarde complète, ainsi que de toutes les sauvegardes incrémentales effectuées jusqu'à la prochaine sauvegarde complète.</p>

<b>gestion centralisée des licences</b>	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. <i>Voir aussi <a href="#">MoM</a>.</i>
<b>gestion de stockage automatique (ASM)</b>	<i>(terme propre à Oracle)</i> Gestionnaire de systèmes de fichiers et de volumes intégré à Oracle qui gère les fichiers de base de données Oracle. Il simplifie la gestion des données et des disques et optimise les performances en fournissant des fonctions de mise en miroir et de répartition sur plusieurs axes.
<b>Gestion de stockage hiérarchique (HSM, pour Hierarchical Storage Management)</b>	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.
<b>Gestionnaire de cellule</b>	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 système de Gestionnaire de cellule.
<b>Gestionnaire de clés</b>	<i>(terme propre à Microsoft Exchange Server)</i> Service Microsoft Exchange Server qui fournit une fonction de cryptage pour une meilleure sécurité. <i>Voir aussi <a href="#">banque d'informations</a> et <a href="#">service de répllication de sites</a>.</i>
<b>gestionnaire de récupération (RMAN)</b>	<i>(terme propre à Oracle)</i> 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.



<b>Gestionnaire RAID P9000 XP (RM)</b>	<i>(terme propre à HP P9000 XP Array Family)</i> L'application Gestionnaire RAID P9000 XP fournit une liste complète de commandes permettant de signaler et de contrôler l'état des applications HP CA P9000 XP et HP BC P9000 XP. Ces commandes communiquent avec l'unité de commande de disque HP StorageWorks P9000 XP Disk Array Family par le biais d'une instance du Gestionnaire RAID P9000 XP. Cette instance convertit les commandes en une séquence de commandes SCSI de bas niveau.
<b>groupe</b>	<i>(terme propre à Microsoft Cluster Server)</i> Ensemble de ressources (par exemple, des volumes de disque, des services d'applications, des noms et adresses IP) nécessaires à l'exécution d'applications compatibles cluster spécifiques.
<b>groupe d'utilisateurs</b>	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 : Admin, Opérateur et Utilisateur.
<b>groupe de disques</b>	<i>(terme propre à Veritas Volume Manager)</i> 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.
<b>groupe de périphériques</b>	<i>(terme propre à EMC Symmetrix)</i> 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.
<b>groupe de réplication de données</b>	<i>(terme propre à HP P6000 EVA Array Family)</i> Regroupement logique de disques virtuels HP P6000 EVA Array Family. Ce groupe peut contenir jusqu'à huit jeux de copies à condition qu'ils aient des caractéristiques communes et partagent un journal HP CA P6000 EVA commun. <i>Voir aussi <a href="#">jeu de copies</a>.</i>

<b>groupe de stockage</b>	<i>(terme propre à Microsoft Exchange Server)</i> 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.
<b>groupe de volumes</b>	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.
<b>HP Business Copy (BC) P6000 EVA</b>	<i>(terme propre à HP P6000 EVA Array Family)</i> Solution logicielle de réplication locale qui permet de créer des copies à un instant donné (répliques) des volumes sources en utilisant les fonctions de snapshot et de clonage du microprogramme P6000 EVA. Voir aussi <a href="#">réplique</a> , <a href="#">volume source</a> , <a href="#">snapshot</a> et <a href="#">HP Continuous Access + Business Copy (CA + BC) P6000 EVA</a> .
<b>HP Business Copy (BC) P9000 XP</b>	<i>(terme propre à HP P9000 XP Array Family)</i> Configuration HP StorageWorks P9000 XP Disk Array Family qui permet de créer et de gérer des copies internes de LDEV à des fins aussi diverses que la sauvegarde et la duplication de données. Les copies (volumes secondaires ou S-VOL) peuvent être séparées des volumes principaux (P-VOLs) et connectées à un système différent. Pour la sauvegarde avec temps d'indisponibilité nul Data Protector, les P-VOL doivent être disponibles pour le système d'application et l'un des jeux de miroirs S-VOL doit être disponible pour le système de sauvegarde. Voir aussi <a href="#">LDEV</a> , <a href="#">HP Continuous Access (CA) P9000 XP</a> , <a href="#">unité de commande principale</a> , <a href="#">système d'application</a> et <a href="#">système de sauvegarde</a> .
<b>HP Continuous Access (CA) P9000 XP</b>	<i>(terme propre à HP P9000 XP Array Family)</i> Configuration HP StorageWorks P9000 XP Disk Array Family qui permet de créer et de gérer des copies distantes de LDEV à des fins aussi diverses que la sauvegarde, la duplication de données et la récupération après sinistre. Les opérations HP CA P9000 XP impliquent les baies de disques principales et distantes (secondaires). Les baies de disques principales sont connectées au système d'application et contiennent les volumes principaux (P-VOL), qui stockent les données d'origine. Les baies de disques secondaires sont

connectées au système de sauvegarde et contiennent les volumes secondaires (S-VOL).

Voir aussi [HP Business Copy \(BC\) P9000 XP](#), [unité de commande principale](#) et [LDEV](#).

**HP Continuous  
Access + Business  
Copy (CA + BC)  
P6000 EVA**

*(terme propre à HP P6000 EVA Array Family)* Configuration HP StorageWorks P6000 EVA Disk Array Family qui permet de créer et de gérer des copies (répliques) des volumes sources sur une baie P6000 EVA distante, puis d'utiliser ces copies comme source pour une réplication locale sur cette baie distante. Voir aussi [HP Business Copy \(BC\) P6000 EVA](#), [réplique](#) et [volume source](#).

**HP StorageWorks  
Command View  
(CV) EVA**

*(terme propre à HP P6000 EVA Array Family)* Interface utilisateur permettant de configurer, de gérer et de surveiller le système de stockage P6000 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 snapshots, de snapclones et de mirrorclones de disques virtuels. Le logiciel HP StorageWorks Command View EVA s'exécute sur le système de gestion du stockage HP. Il est accessible via un navigateur Web. Voir aussi [HP StorageWorks Agent P6000 EVA SMI-S](#) et [fournisseur HP StorageWorks SMI-S P6000 EVA Array](#).

**HP Operations  
Manager**

HP Operations Manager 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 de ce produit de gestion. Cette intégration est mise en œuvre sous la forme d'un module SMART Plug-In pour les serveurs de gestion HP Operations Manager sous Windows, HP-UX, Solaris et Linux. Les versions antérieures de HP Operations Manager se nommaient IT/Operation, Operations Center, Vantage Point Operations et Openview Operations.

**HP Operations  
Manager SMART  
Plug-In (SPI)**

Solution entièrement intégrée et prête à l'emploi qui vient compléter HP Operations Manager, élargissant ainsi le domaine géré. Grâce à l'intégration Data Protector, mise en œuvre 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 de HP Operations Manager.

<b>ICDA</b>	<i>(terme propre à EMC Symmetrix)</i> 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".
<b>ID clé de cryptage-ID Banque</b>	Identificateur combiné utilisé par le serveur gestionnaire de clés Data Protector pour identifier et administrer les clés de cryptage utilisées par Data Protector. <code>IDClé</code> identifie la clé dans la banque de clés. <code>IDBanque</code> identifie la banque de clés dans le Gestionnaire de cellule. Si Data Protector a été mis à niveau à partir d'une version précédente avec la fonctionnalité de cryptage, il se peut que plusieurs <code>IDBanque</code> soient utilisés sur le même Gestionnaire de cellule.
<b>ID d'objet</b>	<i>(terme propre à Windows)</i> 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.
<b>ID de connexion</b>	<i>(terme propre à Microsoft SQL Server)</i> 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 auquel il appartient dans la table système syslogin de Microsoft SQL Server.
<b>ID de sauvegarde</b>	L'identificateur d'un objet d'intégration qui est similaire à l'ID de session de la sauvegarde de l'objet en question. L'ID de sauvegarde est conservé lorsque l'objet est copié, exporté ou importé.
<b>ID de session</b>	Identificateur d'une session de sauvegarde, de restauration, de copie d'objet, de consolidation d'objet, de vérification d'objet ou de gestion de supports, qui est constitué de la date d'exécution de la session et d'un numéro unique.
<b>ID de support de données</b>	Identificateur unique attribué à un support par Data Protector.
<b>IDB</b>	Base de données interne de Data Protector. Il s'agit d'une base de données intégrée résidant sur le Gestionnaire de cellule. Elle contient des informations sur les données sauvegardées, sur les supports utilisés pour la sauvegarde, sur les modalités d'exécution des sessions de sauvegarde, de restauration, etc.,

ainsi que sur les périphériques, bibliothèques et baies de disques configurés.

<b>image DR</b>	Données nécessaires à l'installation et la configuration du système d'exploitation temporaire de récupération après sinistre (DR OS).
<b>importation de supports</b>	Procédé consistant à relire dans la base de données IDB 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. <i>Voir aussi <a href="#">exportation de supports</a>.</i>
<b>index de lecteur</b>	Numéro permettant d'identifier la position mécanique d'un lecteur au sein d'une bibliothèque. Le contrôle robotique utilise ce numéro pour accéder à un lecteur.
<b>Inet</b>	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.
<b>informations d'audit</b>	Données concernant chaque session de sauvegarde effectuée sur une période étendue et définie par l'utilisateur, sur l'ensemble de la cellule Data Protector.
<b>informations de connexion à la base de données cible Oracle</b>	<i>(terme propre à Oracle et SAP R/3)</i> Le format des informations de connexion est le suivant : <i>nom_utilisateur/mot_de_passe@service</i> , où : <ul style="list-style-type: none"><li>• <i>nom_utilisateur</i> 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.</li><li>• <i>mot_de_passe</i> doit correspondre à celui figurant dans le fichier de mots de passe Oracle (<i>orapwd</i>) ; ce fichier permet d'authentifier les utilisateurs chargés de l'administration de la base de données.</li></ul>

- *service* est le nom servant à identifier un processus du serveur SQL\*Net pour la base de données cible.

<b>informations de connexion à la base de données du catalogue de récupération</b>	<i>(terme propre à Oracle)</i> Le format des informations de connexion à la base de données du catalogue de récupération (Oracle) est le suivant : <i>nom_utilisateur/mot de passe@service</i> , 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 <i>service</i> 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.
<b>Informix Server</b>	<i>(terme propre à Informix Server)</i> Fait référence à Informix Dynamic Server.
<b>initialisation</b>	Voir <a href="#">formatage</a> .
<b>instance Oracle</b>	<i>(terme propre à Oracle)</i> 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.
<b>interface de ligne de commande (CLI)</b>	Ensemble de commandes de type DOS et UNIX qui peuvent être utilisées dans les scripts shell pour effectuer des tâches de configuration, de sauvegarde, de restauration et de gestion.
<b>interface de périphérique virtuel</b>	<i>(terme propre à Microsoft SQL Server)</i> Interface de programmation de SQL Server permettant de sauvegarder et de restaurer rapidement des bases de données volumineuses.
<b>Interface utilisateur graphique (GUI)</b>	Interface utilisateur graphique fournie par Data Protector pour offrir un accès aisé 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.
<b>interface XBSA</b>	<i>(terme propre à Informix Server)</i> L'utilitaire ON-Bar et Data Protector communiquent par le biais de l'interface de programmation XBSA (X/Open Backup Services Application).

<b>Internet Information Services (IIS)</b>	<i>(terme propre à Windows)</i> 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).
<b>ISQL</b>	<i>(terme propre à Sybase)</i> Utilitaire Sybase utilisé pour exécuter des tâches d'administration système sur Sybase SQL Server.
<b>Jeu ASR</b>	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 le répertoire <code>données_programme_Data_Protector\Config\Server\dr\asr</code> (Windows Server 2008), <code>répertoire_Data_Protector\Config\Server\dr\asr</code> (autres systèmes Windows) ou <code>/etc/opt/omni/server/dr/asr</code> (systèmes UNIX) ainsi que sur le support de sauvegarde. Après un sinistre, le fichier archive ASR est extrait sur des disquettes dont vous aurez besoin pour exécuter le processus de récupération automatique du système.
<b>jeu de copies</b>	<i>(terme propre à HP P6000 EVA Array Family)</i> Paire constituée des volumes sources sur une baie P6000 EVA locale et de leur réplique sur une baie P6000 EVA distante. Voir aussi <a href="#">volume source, réplique</a> et <a href="#">HP Continuous Access + Business Copy (CA + BC) P6000 EVA</a>
<b>jeu de copies miroir</b>	<i>(terme propre à Microsoft VSS)</i> Ensemble de copies miroir créées au même instant. Voir aussi <a href="#">copie miroir</a> et <a href="#">jeu de répliques</a> .
<b>jeu de répliques</b>	<i>(terme propre à ZDB)</i> Groupe de répliques, toutes créées en utilisant la même spécification de sauvegarde. Voir aussi <a href="#">réplique</a> et <a href="#">rotation des jeux de répliques</a> .
<b>jeu de sauvegarde</b>	Jeu complet d'objets d'intégration associés à une sauvegarde.
<b>jeu de sauvegarde</b>	<i>(terme propre à Oracle)</i> Regroupement logique de fichiers sauvegardés 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 des fichiers de données ou des journaux d'archive, mais pas les deux à la fois.

**jeu de supports**

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.

**jonction de répertoire**

*(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.

**journal d'événements (journal d'événements Data Protector)**

Référentiel central de l'ensemble des notifications ayant trait à Data Protector. Par défaut, toutes les notifications sont envoyées au journal d'événements. Les événements sont consignés sur le Gestionnaire de cellule dans le fichier `données_programme_Data_Protector\log\server\Ob2EventLog.txt` (Windows Server 2008), `répertoire_Data_Protector\log\server\Ob2EventLog.txt` (autres systèmes Windows) ou `/var/opt/omni/server/log/Ob2EventLog.txt` (systèmes UNIX). Le journal d'événements n'est accessible qu'aux utilisateurs appartenant au groupe Admin de Data Protector et à ceux qui disposent des droits utilisateur `Rapports` et `notifications` Data Protector. Vous pouvez afficher ou supprimer l'ensemble des événements du journal.

**journal de rétablissement**

*(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.

**journal de rétablissement archivé**

*(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 ne sont pas archivés.

Voir aussi [journal de rétablissement en ligne](#).

### **journal de rétablissement en ligne**

Voir [journal de rétablissement archivé](#).

### **journal de rétablissement en ligne**

*(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](#).

### **Journal des modifications**

*(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.

### **journaux d'audit**

Fichiers de données dans lesquels les informations d'audit sont stockées.

### **journaux d'événements**

*(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.

### **journaux de transactions**

*(terme propre à Data Protector)* Assure 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 l'IDB et nécessaires à sa récupération.

<b>keychain</b>	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.
<b>KMS</b>	Le serveur gestionnaire de clés (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. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.
<b>LBO</b>	<i>(terme propre à EMC Symmetrix)</i> 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.
<b>LCR (local continuous replication)</b>	<i>(terme propre à Microsoft Exchange Server)</i> La réplication continue locale (LCR, pour Local Continuous Replication) 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 en tant que 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. <i>Voir aussi <a href="#">Cluster Continuous Replication</a> et <a href="#">service de réplication Exchange</a>.</i>

<b>LDEV</b>	<i>(terme propre à HP P9000 XP Array Family)</i> Partition logique d'un disque physique d'une baie de disques HP StorageWorks P9000 XP Disk Array Family. Le LDEV est l'entité qui peut être répliquée à l'aide de la fonctionnalité Split Mirror ou Snapshot de la baie de disques. Voir aussi <a href="#">HP Business Copy (BC) P9000 XP</a> , <a href="#">HP Continuous Access (CA) P9000 XP</a> et réplique.
<b>lecteur</b>	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.
<b>liste de préallocation</b>	Dans un pool de supports, sous-ensemble de supports définissant l'ordre dans lequel les supports sont utilisés pour la sauvegarde.
<b>LISTENER.ORA</b>	<i>(terme propre à Oracle)</i> Fichier de configuration Oracle décrivant un ou plusieurs listeners TNS (Transparent Network Substrate) sur un serveur.
<b>make_net_recovery</b>	<code>make_net_recovery</code> est une commande Ignite-UX qui permet de créer une archive 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 <code>make_boot_tape</code> ou lorsque le système démarre directement à partir du serveur Ignite-UX. Vous pouvez automatiser le démarrage direct via le serveur Ignite-UX à l'aide de la commande Ignite-UX <code>bootsys</code> ou le spécifier en mode interactif sur la console d'amorçage.
<b>make_tape_recovery</b>	<code>make_tape_recovery</code> 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.
<b>Manager-of-Managers (MoM)</b>	Voir <a href="#">MoM</a> .

<b>MAPI</b>	<i>(terme propre à Microsoft Exchange server)</i> L'interface MAPI (Messaging Application Programming Interface) est l'interface de programmation qui permet aux applications et aux clients de messagerie de communiquer avec les systèmes de messagerie et d'information.
<b>MCU</b>	Voir <a href="#">unité de commande principale (MCU, pour Main Control Unit)</a> .
<b>Microsoft Exchange Server</b>	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.
<b>Microsoft Management Console (MMC)</b>	<i>(terme propre à Windows)</i> 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.
<b>Microsoft SQL Server</b>	Système de gestion de base de données destiné à répondre aux besoins du traitement distribué "client-serveur".
<b>Microsoft Volume Shadow Copy Service (VSS)</b>	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, les fournisseurs de copie miroir et le noyau du système d'exploitation pour permettre la gestion des copies miroir des volumes et des jeux de copies. Voir aussi <a href="#">copie miroir</a> , <a href="#">fournisseur de copie miroir</a> , <a href="#">réplique</a> et <a href="#">module d'écriture</a> .
<b>miroir d'objet</b>	Copie d'un objet sauvegarde créé à l'aide de la mise en miroir d'objet. Les miroirs d'objets sont souvent appelés des copies d'objets.

<b>miroir de premier niveau</b>	<p>(terme propre à HP P9000 XP Array Family) Miroir d'un disque interne (LDEV) d'une baie de disques HP StorageWorks P9000 XP Disk Array Family qui peut être lui-même mis en mémoire pour produire des miroirs de second niveau. Pour les tâches de restauration instantanée et de sauvegarde avec temps d'indisponibilité nul Data Protector, vous pouvez seulement utiliser des miroirs de premier niveau.</p> <p>Voir aussi <a href="#">volume principal</a> et <a href="#">numéro d'unité miroir (MU)</a>.</p>
<b>miroir (terme propre à EMC Symmetrix et à HP P9000 XP Array Family)</b>	<p>Voir <a href="#">volume cible</a>.</p>
<b>mirrorclone</b>	<p>(terme propre à HP P6000 EVA Array Family) Réplique dynamique d'un volume de stockage, qui est constamment mise à jour en fonction des modifications apportées au volume de stockage d'origine par le biais d'un lien de réplication locale. La réplication entre le volume de stockage d'origine et son mirrorclone peut être suspendue. Pour chaque volume de stockage, il est possible de créer un mirrorclone unique sur la baie de disques.</p>
<b>mise au coffre de supports</b>	<p>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.</p>
<b>Mise en miroir LVM</b>	<p>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.</p>
<b>MMD</b>	<p>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.</p>

<b>MMDB</b>	<p>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.</p> <p>Voir aussi <a href="#">CMMDB</a> et <a href="#">CDB</a>.</p>
<b>mode compatible VSS</b>	<p><i>(terme propre au fournisseur HP P9000 XP Array Family VSS)</i></p> <p>L'un des deux modes de fonctionnement du fournisseur matériel P9000 XP Array VSS. Lorsque le fournisseur P9000 XP Array est en mode compatible VSS, le volume source (P-VOL) et sa réplique (S-VOL) sont en mode simplex et dissociés après une sauvegarde. Par conséquent, le nombre de répliques (S-VOL par P-VOL) en rotation n'est pas limité. Pour ce type de configuration, la restauration à partir d'une sauvegarde est possible uniquement par le biais d'un changement de disques.</p> <p>Voir aussi <a href="#">mode resynchronisation</a>, <a href="#">volume source</a>, <a href="#">volume principal (P-VOL)</a>, <a href="#">réplique</a>, <a href="#">volume secondaire (S-VOL)</a> et <a href="#">rotation des jeux de répliques</a>.</p>
<b>mode resynchronisation</b>	<p><i>(terme propre au fournisseur HP P9000 XP Array Family VSS)</i></p> <p>L'un des deux modes de fonctionnement du fournisseur matériel P9000 XP Array VSS. Lorsque le fournisseur P9000 XP Array est en mode resynchronisation, le volume source (P-VOL) et sa réplique (S-VOL) sont en relation de miroir suspendue 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.</p> <p>Voir aussi <a href="#">mode compatible VSS</a>, <a href="#">volume source</a>, <a href="#">volume principal (P-VOL)</a>, <a href="#">réplique</a>, <a href="#">volume secondaire (S-VOL)</a>, <a href="#">numéro d'unité miroir (MU)</a> et <a href="#">rotation des jeux de répliques</a>.</p>
<b>module d'écriture</b>	<p><i>(terme propre à Microsoft VSS)</i> Processus initiant la modification des données sur le volume d'origine. Les modules d'écriture sont généralement des applications ou des services système rédigeant des informations permanentes sur un volume. Ils participent également au processus de synchronisation des copies miroir en assurant la cohérence des données.</p>

<b>module fournisseur d'informations sur les modifications</b>	<i>(terme propre à Windows)</i> Module pouvant être interrogé pour déterminer quels objets d'un système de fichiers ont été créés, modifiés ou supprimés.
<b>MoM</b>	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.
<b>moteur de stockage extensible (ESE, pour Extensible Storage Engine)</b>	<i>(terme propre à Microsoft Exchange Server)</i> Technologie de base de données servant de système de stockage pour les échanges d'informations avec le serveur Microsoft Exchange.
<b>MSM</b>	Le Gestionnaire de session de supports (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.
<b>niveau de journalisation</b>	Le niveau de journalisation indique le nombre de détails concernant les fichiers et répertoires qui sont écrits dans la base de données interne (IDB) pendant la sauvegarde, la copie ou la consolidation d'objets. 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 l'IDB, la vitesse de sauvegarde et la facilité d'exploration des données à restaurer.
<b>nom de verrouillage</b>	Vous pouvez configurer plusieurs fois le même périphérique physique avec des caractéristiques différentes en utilisant des noms de périphérique distincts. 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 périphériques utilisant le même périphérique physique.

<b>numéro d'unité miroir (MU)</b>	<i>(terme propre à HP P9000 XP Array Family)</i> Nombre entier non négatif qui détermine un volume secondaire (S-VOL) d'un disque interne (LDEV) situé sur une baie de disques HP StorageWorks P9000 XP Disk Array Family. Voir aussi <a href="#">miroir de premier niveau</a> .
<b>obdrindex.dat</b>	Voir <a href="#">fichier de récupération de l'IDB</a> .
<b>objet</b>	Voir <a href="#">objet sauvegarde</a> .
<b>objet d'intégration</b>	Un objet sauvegarde d'une intégration Data Protector, telle que Oracle ou SAP DB.
<b>objet sauvegarde</b>	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 : <ul style="list-style-type: none"> <li>• Nom de client : nom d'hôte du client Data Protector dans lequel l'objet sauvegarde est hébergé.</li> <li>• 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.</li> <li>• 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).</li> <li>• Type : Type de l'objet sauvegarde. Pour les objets système de fichiers — type de système de fichiers (WinFS, par exemple). Pour les objets intégration — "Bar".</li> </ul>
<b>objet, copie</b>	Processus de copie des 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.
<b>objets, mise en miroir</b>	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.

### **ON-Bar**

*(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.

### **ONCONFIG**

*(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).

### **opérateurs booléens**

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 identique à récupération AND après AND sinistre AND manuelle.

### **opération hors contrôle ou sans surveillance**

Sauvegarde ou restauration ayant lieu en dehors des heures normales de bureau, ce qui signifie qu'aucun opérateur n'est présent pour utiliser l'application de sauvegarde ou les demandes de montage de service, par exemple.

### **opération sans surveillance**

Voir [opération hors contrôle](#).

<b>Oracle Data Guard</b>	<i>(terme propre à Oracle)</i> 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.
<b>ORACLE_SID</b>	<i>(terme propre à Oracle)</i> Nom unique pour une instance de serveur Oracle. Pour passer d'un serveur Oracle à un autre, spécifiez le ORACLE_SID voulu. Le ORACLE_SID est inséré dans les parties CONNECT DATA du descripteur de connexion d'un fichier TNSNAMES.ORA et dans la définition du listener TNS du fichier LISTENER.ORA.
<b>package</b>	<i>(terme propre à MC/ServiceGuard et Veritas Cluster)</i> Ensemble de ressources (par exemple, groupes de volumes, services d'applications, noms et adresses IP) nécessaires à l'exécution d'applications compatibles cluster spécifiques.
<b>paquet magique</b>	Voir <a href="#">Wake ONLAN</a> .
<b>parallélisme</b>	Concept consistant à lire plusieurs flux de données depuis une base de données en ligne.
<b>parallélisme de bases de données</b>	Plusieurs bases de données sont sauvegardées en même temps si le nombre de périphériques disponibles permet d'effectuer des sauvegardes en parallèle.
<b>parcours de l'arborescence de fichiers</b>	<i>(terme propre à Windows)</i> Processus consistant à parcourir un système de fichiers pour déterminer quels objets ont été créés, modifiés ou supprimés.
<b>partage de charge</b>	Par défaut, Data Protector équilibre automatiquement la charge (l'utilisation) des périphériques sélectionnés pour la sauvegarde, afin que ces derniers soient utilisés de manière uniforme. Ce procédé permet d'optimiser l'utilisation des périphériques en

équilibrant le nombre d'objets écrits sur chacun. Cette opération s'effectue automatiquement pendant la sauvegarde ; vous ne devez donc pas 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 la spécification de sauvegarde. Data Protector accèdera aux périphériques dans l'ordre spécifié.

<b>passage</b>	Voir <a href="#">basculement</a> .
<b>périphérique</b>	Unité physique contenant soit un lecteur, soit une unité plus complexe (une bibliothèque par exemple).
<b>périphérique cible (R2)</b>	<i>(terme propre à EMC Symmetrix)</i> 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 <a href="#">périphérique source (R1)</a> .
<b>périphérique compatible OBDR</b>	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.
<b>périphérique de bibliothèque de fichiers</b>	Périphérique résidant sur un disque qui fonctionne comme une bibliothèque avec plusieurs supports et contient donc plusieurs fichiers appelés dépôts de fichier.
<b>périphérique de bibliothèque de stockage</b>	Périphérique composé de plusieurs emplacements destinés à stocker des supports optiques ou des 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".
<b>périphérique de bibliothèque de stockage de fichiers</b>	Périphérique résidant sur un disque et constitué de plusieurs emplacements utilisés pour le stockage de fichiers.

<b>périphérique de fichier autonome</b>	Un périphérique de fichier est un fichier dans un répertoire spécifié vers lequel vous sauvegardez des données.
<b>périphérique de sauvegarde</b>	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.
<b>périphérique en mode continu</b>	On dit d'un périphérique qu'il fonctionne en mode continu s'il peut fournir un volume de données suffisant au support pour que ce dernier fonctionne 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.
<b>périphérique physique</b>	Unité physique contenant soit un lecteur, soit une unité plus complexe (une bibliothèque par exemple).
<b>périphérique source (R1)</b>	<i>(terme propre à EMC Symmetrix)</i> 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) d'une unité EMC Symmetrix distante. Tout périphérique R1 doit être affecté à un type de groupe RDF1. <i>Voir aussi <a href="#">périphérique cible (R2)</a>.</i>
<b>phase 0 de la récupération après sinistre</b>	Préparation à la récupération après sinistre. Il s'agit d'une condition préalable à la réussite de la récupération après sinistre.
<b>phase 1 de la récupération après sinistre</b>	Installation et configuration du DR OS (système d'exploitation de récupération après sinistre) visant à établir la structure de stockage existant précédemment.
<b>phase 2 de la récupération après sinistre</b>	Restauration du système d'exploitation (avec toutes les données de configuration qui définissent l'environnement) et de Data Protector.

<b>phase 3 de la récupération après sinistre</b>	Restauration des données utilisateur et d'application.
<b>Planificateur</b>	Fonction permettant de contrôler le moment et la fréquence des sauvegardes automatiques. En configurant une planification, vous pouvez automatiser le lancement des sauvegardes.
<b>point d'analyse</b>	<i>(terme propre à Windows)</i> 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 tente de trouver le filtre de système de fichiers associé au format des données.
<b>point de montage</b>	Point d'accès à un disque ou à un volume logique dans une structure de répertoires, par exemple <code>/opt</code> ou <code>d:</code> . Sous UNIX, les points de montage sont accessibles au moyen de la commande <code>bdf</code> ou <code>df</code> .
<b>point de montage de volume</b>	<i>(terme propre à Windows)</i> 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.
<b>Pont FC</b>	Voir <a href="#">Pont Fibre Channel</a> .
<b>Pont Fibre Channel</b>	Un pont 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 du pont ou multiplexeur. Des ports SCSI parallèles se trouvent à l'autre extrémité. La passerelle permet le transfert des paquets SCSI entre les périphériques Fibre Channel et SCSI parallèles.

<b>pool de supports</b>	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.
<b>pool libre</b>	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.
<b>pool smart copy</b>	<i>(terme propre à VLS)</i> 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 <a href="#">Système de bibliothèque virtuelle (VLS)</a> et <a href="#">copie intelligente</a> .
<b>post-exécution</b>	Option de sauvegarde qui exécute une commande ou un script après la sauvegarde d'un objet ou une fois que la session de sauvegarde est terminée. Les commandes de 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 <a href="#">pré-exécution</a> .
<b>pré-exécution</b>	Option de sauvegarde qui exécute une commande ou un script avant la sauvegarde d'un objet ou avant que la session de sauvegarde ne démarre. Les commandes de 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 <a href="#">post-exécution</a> .
<b>processus BC</b>	<i>(terme propre à EMC Symmetrix)</i> 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 <a href="#">BCV</a> .
<b>Profil utilisateur</b>	<i>(terme propre à Windows)</i> Informations de configuration définies pour chaque utilisateur. Ces informations comprennent la configuration du bureau, les couleurs d'écran, les connexions réseau, etc. Lorsqu'un utilisateur se connecte, le système charge son profil et l'environnement Windows le prend en compte.

<b>propriétaire de la sauvegarde</b>	Tout objet sauvegarde de la base de données IDB a un propriétaire. Par défaut, le propriétaire d'une sauvegarde est l'utilisateur qui lance la session de sauvegarde.
<b>propriété</b>	<p>La propriété de sauvegarde agit sur la capacité des utilisateurs à voir et à restaurer les données. Chaque session de sauvegarde, avec toutes les données sauvegardées qu'elle contient, est affectée à un propriétaire. Il peut s'agir de l'utilisateur qui lance une sauvegarde interactive, du compte sous lequel le processus CRS est exécuté ou de l'utilisateur désigné comme propriétaire dans les options de la spécification de sauvegarde.</p> <p>Si un utilisateur démarre une spécification de sauvegarde existante sans la modifier, la session n'est pas considérée comme interactive.</p> <p>Si une spécification de sauvegarde modifiée est démarrée par un utilisateur, celui-ci est le propriétaire, à moins que les conditions ci-après soient remplies :</p> <ul style="list-style-type: none"> <li>• L'utilisateur possède le droit utilisateur Permuter propriété de session.</li> <li>• Le propriétaire d'une session de sauvegarde est explicitement défini dans la spécification de sauvegarde, avec le nom d'utilisateur, le groupe, le nom de domaine et le nom du système.</li> </ul> <p>Si vous prévoyez d'effectuer une sauvegarde sur un Gestionnaire de cellule UNIX, le propriétaire de la session est root:sys à moins que les conditions indiquées ci-dessus ne soient remplies.</p> <p>Si vous prévoyez d'effectuer une sauvegarde sur un Gestionnaire de cellule Windows, le propriétaire de la session est l'utilisateur spécifié lors de l'installation, à moins que les conditions indiquées ci-dessus soient remplies.</p> <p>Lors de la copie ou de la consolidation d'objets, le propriétaire est par défaut l'utilisateur qui démarre l'opération, sauf si un autre propriétaire est défini dans la spécification de copie ou de consolidation.</p>
<b>protection</b>	Voir <a href="#">protection des données</a> et également <a href="#">protection de catalogue</a> .
<b>protection de catalogue</b>	<p>Permet de définir le temps de conservation des informations concernant les données sauvegardées (noms et versions de fichiers) dans la base de données IDB.</p> <p>Voir aussi <a href="#">protection des données</a>.</p>

<b>pulsation</b>	Ensemble de données de cluster qui comporte un horodatage contenant des informations sur l'état de fonctionnement d'un nœud de cluster spécifique. Cet ensemble de données est distribué à tous les nœuds de cluster.
<b>quota de disque</b>	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.
<b>quotas de disque utilisateur</b>	Le support de gestion des quotas NTFS permet le contrôle et le suivi élaboré de l'utilisation de l'espace disque sur les volumes de stockage partagés. Data Protector sauvegarde des quotas de disque utilisateur sur l'ensemble du système et pour tous les utilisateurs configurés à un instant donné.
<b>RAID</b>	Ensemble redondant de disques indépendants (Redundant Array of Independent Disks).
<b>rapport d'audit</b>	Sortie lisible par l'utilisateur d'informations d'audit créées à partir des données stockées dans les fichiers journaux d'audit.
<b>RCU</b>	Voir <a href="#">Unité de télécommande (RCU)</a> .
<b>RDF1/RDF2</b>	<i>(terme propre à EMC Symmetrix)</i> 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).
<b>RDS</b>	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.
<b>RecoveryInfo</b>	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.
<b>récupération après sinistre</b>	Procédé 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.



<b>récupération en ligne</b>	La récupération en ligne s'exécute lorsque le Gestionnaire de cellule est accessible. Dans ce cas, la plupart des fonctionnalités de Data Protector sont disponibles (le Gestionnaire de cellule exécute la session, les sessions de restauration sont consignées dans l'IDB, vous pouvez suivre l'avancement de la restauration via l'interface utilisateur, etc.).
<b>récupération hors ligne</b>	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.
<b>récupération locale et distante</b>	La récupération distante s'effectue lorsque tous les hôtes de l'Agent de support spécifiés dans le fichier SRD 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.
<b>récupération matérielle</b>	<i>(terme propre à Microsoft Exchange Server)</i> Récupération de la base de données Microsoft Exchange Server effectuée après une restauration par le moteur de base de données, au moyen des fichiers journaux de transactions.
<b>recyclage ou suppression de la protection</b>	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 enregistrées sur le support.
<b>réécriture</b>	Option définissant un mode de résolution de conflits pendant la restauration. Tous les fichiers sauvegardés sont restaurés, même s'ils sont plus anciens que les fichiers existants. <i>Voir aussi <a href="#">fusion</a>.</i>

<b>Registre Windows</b>	Base de données centralisée utilisée par Windows pour stocker les informations de configuration du système d'exploitation et des applications installées.
<b>répertoire DC</b>	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 <code>dcbf</code> et se trouve sur le Gestionnaire de cellule, dans le répertoire <code>données_programme_Data_Protector\db40</code> (Windows Server 2008), <code>répertoire_Data_Protector\db40</code> (autres systèmes Windows) ou <code>/var/opt/omni/server/db40</code> (systèmes UNIX). Vous pouvez cependant en créer davantage et utiliser un emplacement de votre choix. Chaque cellule peut gérer jusqu'à 50 répertoires DC. Par défaut, la taille maximale d'un répertoire DC est de 16 Go.
<b>répertoire_Data_Protector</b>	Sous Windows Vista, Windows 7 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 <code>%ProgramFiles%\OmniBack</code> , mais vous pouvez le modifier dans l'assistant d'installation de Data Protector au moment de l'installation. Voir aussi <a href="#">données_programme_Data_Protector</a> .
<b>réplique</b>	<i>(terme propre à ZDB)</i> Une image, à un instant T, des données des volumes sources qui contiennent les objets sauvegarde spécifiques 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 <a href="#">snapshot</a> , <a href="#">création de snapshot</a> , <a href="#">split mirror</a> et <a href="#">création de split mirror</a> .

**restauration  
incrémentale**

*(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.

**restauration  
instantanée**

*(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. Selon l'application ou la base de données concernée, ce processus est suffisant, ou d'autres étapes peuvent être nécessaires pour une récupération complète, par exemple l'application de fichiers journaux de transactions.  
*Voir aussi [réplique](#), [sauvegarde avec temps d'indisponibilité nul \(ZDB\)](#), [sauvegarde ZDB sur disque](#) et [sauvegarde ZDB sur disque + bande](#).*

**restauration  
parallèle**

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.

<b>restauration Split Mirror</b>	<i>(terme propre à EMC Symmetrix et à HP P9000 XP Array Family)</i> Processus dans lequel les données sauvegardées lors d'une session de sauvegarde ZDB sur bande ou ZDB sur disque + bande sont d'abord copiées à partir des supports de sauvegarde vers une réplique, puis à partir de la réplique vers les volumes sources. Les objets sauvegarde individuels ou les sessions complètes peuvent être restauré(e)s à l'aide de cette méthode. Voir aussi <a href="#">sauvegarde ZDB sur bande</a> , <a href="#">ZDB sur disque + bande</a> et <a href="#">réplique</a> .
<b>RMAN (terme propre à Oracle)</b>	Voir <a href="#">Gestionnaire de récupération</a> .
<b>rotation des jeux de répliques</b>	<i>(terme propre à ZDB)</i> Utilisation d'un jeu de répliques pour la génération régulière de sauvegardes : chaque fois qu'une même spécification de sauvegarde nécessitant l'utilisation d'un jeu de répliques est exécutée, une nouvelle réplique est créée puis ajoutée au jeu, tant que le nombre maximum de répliques fixé pour le jeu n'est pas atteint. Une fois ce nombre atteint, la réplique la plus ancienne du jeu est écrasée. Voir aussi <a href="#">réplique</a> et <a href="#">jeu de répliques</a> .
<b>rotation des miroirs (terme propre à HP P9000 XP Array Family)</b>	Voir <a href="#">rotation des jeux de répliques</a> .
<b>RSM</b>	Le Gestionnaire de session de restauration (Restore Session Manager) Data Protector contrôle les sessions de restauration et de vérification d'objet. Ce processus est toujours exécuté sur le système du Gestionnaire de cellule.
<b>RSM</b>	<i>(terme propre à Windows)</i> 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.
<b>SAPDBA</b>	<i>(terme propre à SAP R/3)</i> Interface utilisateur SAP R/3 intégrant les outils BRBACKUP, BRARCHIVE et BRRESTORE.

<b>sauvegarde avec temps d'indisponibilité nul (ZDB)</b>	<p>Approche de sauvegarde selon laquelle les techniques de duplication des données fournies par une baie de disques permettent de 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.</p> <p>Voir aussi <a href="#">sauvegarde ZDB sur disque</a>, <a href="#">sauvegarde ZDB sur bande</a>, <a href="#">ZDB sur disque + bande</a> et <a href="#">restauration instantanée</a>.</p>
<b>sauvegarde complète</b>	<p>Sauvegarde au cours de laquelle tous les objets sélectionnés sont sauvegardés, qu'ils aient été ou non modifiés récemment.</p> <p>Voir aussi <a href="#">types de sauvegarde</a>.</p>
<b>sauvegarde complète synthétique</b>	<p>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.</p>
<b>sauvegarde complète virtuelle</b>	<p>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.</p>
<b>sauvegarde d'image disque (rawdisk)</b>	<p>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.</p>
<b>sauvegarde de base de données complète</b>	<p>Sauvegarde de toutes les données d'une base de données, et non uniquement des données ayant été modifiées après la dernière sauvegarde (complète ou incrémentale) de la base de données. Une sauvegarde complète de base de données ne dépend d'aucune autre sauvegarde.</p>

**sauvegarde de base de données différentielle**

Sauvegarde de base de données au cours de laquelle ne sont sauvegardées que les modifications intervenues après la dernière sauvegarde complète de la base.

**sauvegarde de boîte aux lettres complète**

La sauvegarde complète de boîte aux lettres consiste à sauvegarder tout le contenu d'une boîte aux lettres.

**sauvegarde de client**

Sauvegarde de tous les volumes (systèmes de fichiers) montés sur un client Data Protector. Ce qui est sauvegardé est fonction du mode de sélection des objets dans une spécification de sauvegarde :

- Si vous cochez la case située en regard du nom du système client, un objet sauvegarde unique de type `système client` est créé. Par conséquent, lors de la sauvegarde, Data Protector détecte d'abord tous les volumes montés sur le client sélectionné, puis les sauvegarde. Sur les clients Windows, la `CONFIGURATION` est également sauvegardée.
- Si vous sélectionnez individuellement tous les volumes montés sur le système client, un objet sauvegarde séparé de type `Système de fichiers` est créé pour chaque volume. Ainsi, au moment de la sauvegarde, seuls les volumes sélectionnés sont sauvegardés. Les volumes qui ont été potentiellement montés sur le client après la création de la spécification de sauvegarde ne sont pas sauvegardés.

**sauvegarde de configuration Windows**

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.

**sauvegarde de disque en plusieurs étapes**

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. La procédure consiste à sauvegarder les données sur un type de support (par exemple, un disque), puis à les copier vers un autre type de support (par exemple, une bande).

**sauvegarde de snapshot**

Voir [sauvegarde sur bande ZDB](#), [sauvegarde sur disque ZDB](#) et [sauvegarde sur disque+bande ZDB](#).

<b>sauvegarde de transaction</b>	Les sauvegardes de transaction consomment 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.
<b>sauvegarde de transaction</b>	<i>(terme propre à Sybase et SQL)</i> Sauvegarde du journal de transactions contenant un enregistrement des modifications effectuées depuis la dernière sauvegarde complète ou la dernière sauvegarde de transaction.
<b>sauvegarde delta</b>	Sauvegarde contenant toutes les modifications apportées à la base de données depuis la dernière sauvegarde, quel qu'en soit le type. Voir aussi <a href="#">types de sauvegarde</a> .
<b>sauvegarde différentielle</b>	Sauvegarde incrémentale qui permet de sauvegarder les modifications effectuées depuis la dernière sauvegarde complète. Pour procéder à une telle sauvegarde, indiquez le type de sauvegarde Incr1. Voir aussi <a href="#">sauvegarde incrémentale</a> .
<b>sauvegarde différentielle</b>	<i>(terme propre à Microsoft SQL Server)</i> Sauvegarde de base de données au cours de laquelle seules les modifications intervenues après la dernière sauvegarde complète de la base sont sauvegardées. Voir aussi <a href="#">types de sauvegarde</a> .
<b>sauvegarde du journal des transactions</b>	Les sauvegardes du journal des transactions consomment 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.
<b>sauvegarde en ligne</b>	Une sauvegarde effectuée alors que la base de données est accessible. La base de données passe dans un mode de sauvegarde particulier pendant toute la durée du processus de réplication des données. Pour les sauvegardes sur bande, par exemple, elle est nécessaire jusqu'à ce que le transfert de données vers la bande soit terminé. Pendant ce laps de temps,

la base de données continue à être pleinement opérationnelle mais des problèmes de performance mineurs peuvent survenir et la taille des fichiers journaux peut croître très rapidement. Elle reprend son fonctionnement normal avant que les opérations post-sauvegarde potentielles ne démarrent. 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](#).*

**sauvegarde hors ligne**

Sauvegarde au cours de laquelle une base de données d'application ne peut pas être utilisée par l'application. Lors d'une session de sauvegarde hors ligne, 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 durée du processus de réplication des données. Pour les sauvegardes sur bande, par exemple, cette mise en veille est effective jusqu'à ce que le transfert de données vers la bande soit terminé. Elle reprend son fonctionnement normal avant que les opérations post-sauvegarde potentielles ne démarrent.  
*Voir aussi [sauvegarde avec temps d'indisponibilité nul \(ZDB\)](#) et [sauvegarde en ligne](#).*

**sauvegarde incrémentale**

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](#).*

**sauvegarde incrémentale**

*(terme propre à Microsoft Exchange Server)* Sauvegarde de données Microsoft Exchange Server modifiées depuis la dernière sauvegarde complète ou incrémentale. Avec la sauvegarde incrémentale, seuls les fichiers journaux de transactions sont sauvegardés.  
*Voir aussi [types de sauvegarde](#).*

**sauvegarde incrémentale avancée**

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.



<b>sauvegarde incrémentale de boîte aux lettres</b>	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.
<b>sauvegarde incrémentale de boîte aux lettres "incrémentale 1"</b>	Une sauvegarde incrémentale <sup>1</sup> de boîte aux lettres consiste à sauvegarder toutes les modifications apportées à la boîte aux lettres depuis la dernière sauvegarde complète.
<b>sauvegarde rawdisk</b>	Voir <a href="#">sauvegarde d'image disque</a> .
<b>sauvegarde sans bande (terme propre à ZDB)</b>	Voir <a href="#">ZDB sur disque</a> .
<b>sauvegarde Split Mirror (terme propre à EMC Symmetrix)</b>	Voir <a href="#">ZDB sur bande</a> .
<b>sauvegarde Split Mirror (terme propre à HP P9000 XP Array Family)</b>	Voir <a href="#">sauvegarde sur bande ZDB</a> , <a href="#">sauvegarde sur disque ZDB</a> et <a href="#">sauvegarde sur disque+bande ZDB</a> .
<b>sauvegarde synthétique</b>	Solution de sauvegarde qui produit une sauvegarde complète synthétique, équivalant à une sauvegarde complète classique en termes de données, sans créer de charge sur 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.
<b>sauvegarde système sur bande</b>	( <i>terme propre à Oracle</i> ) Interface Oracle chargée d'exécuter les actions nécessaires au chargement, à l'étiquetage et au déchargement des bons périphériques de sauvegarde lorsqu'Oracle émet des demandes de sauvegarde ou de restauration.
<b>sauvegarde ZDB complète</b>	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](#).

**sauvegarde ZDB  
incrémentale**

Session de sauvegarde de système de fichiers ZDB (avec temps d'indisponibilité nul) sur bande ou sur disque et bande qui ne copie sur le support que les modifications effectuées depuis la dernière sauvegarde protégée (complète ou incrémentale).

Voir aussi [sauvegarde ZDB complète](#).

**sauvegarde ZDB  
sur bande**

*(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. Avec certaines familles de baies de disques, la restauration Split Mirror peut aussi être utilisée.

Voir aussi [sauvegarde avec temps d'indisponibilité nul \(ZDB\)](#), [sauvegarde ZDB sur disque](#), [sauvegarde ZDB sur disque + bande](#), [restauration instantanée](#) et [réplique](#).

**sauvegarde ZDB  
sur disque**

*(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 sources 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. Le processus de restauration instantanée permet de restaurer une réplique à partir d'une session ZDB sur disque.

Voir aussi [sauvegarde avec temps d'indisponibilité nul \(ZDB\)](#), [sauvegarde ZDB sur bande](#), [ZDB sur disque + bande](#), [restauration instantanée](#) et [rotation des jeux de répliques](#).

**sauvegarde ZDB  
sur disque +  
bande**

*(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 sources à un instant donné, de la même manière que la sauvegarde 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 avec certaines familles de baies de disques, la restauration Split Mirror. Voir aussi [sauvegarde avec temps d'indisponibilité nul \(ZDB\)](#), [sauvegarde ZDB sur disque](#), [sauvegarde ZDB sur bande](#), [restauration instantanée](#), [réplique](#) et [rotation des jeux de répliques](#).

**script CMD pour Informix Server**

(*terme propre à Informix Server*) Script CMD Windows créé dans INFORMIXDIR lorsqu'une base de données Informix Server est configurée. Le script CMD est un ensemble de commandes système chargé d'exporter les variables d'environnement pour Informix Server.

**script shell log\_full**

(*terme propre à Informix Server UNIX*) Script fourni par ON-Bar que vous pouvez 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 REP\_INFORMIX/etc/no\_log.sh au paramètre de configuration ALARMPROGRAM.

**section PME/PMI**

Voir [sauvegarde Split Mirror](#).

**serveur d'interface Java**

Le serveur de l'interface Java est un composant de l'interface utilisateur graphique Java qui est installé sur le système Gestionnaire de cellule de 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.

**serveur de base de données**

Ordinateur sur lequel est stockée une base de données volumineuse, telle qu'une base de données SAP R/3 ou Microsoft SQL. Une base de données stockée sur un serveur est accessible aux clients.

<b>serveur DHCP</b>	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.
<b>Serveur d'installation</b>	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 : l'un pour les systèmes UNIX et l'autre pour les systèmes Windows.
<b>Serveur DNS</b>	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.
<b>serveur Sybase SQL</b>	<i>(terme propre à Sybase)</i> 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.
<b>serveur virtuel</b>	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 nœud de cluster spécifique.
<b>serveur WINS</b>	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.
<b>Service de réplication de fichiers (FRS)</b>	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.

<b>service de répllication de sites</b>	<i>(terme propre à Microsoft Exchange Server)</i> Service Microsoft Exchange Server 2003 qui offre une compatibilité avec Microsoft Exchange Server 5.5 par l'émulation du service d'annuaire Exchange Server 5.5. Voir aussi <a href="#">banque d'informations</a> et <a href="#">service Gestionnaire de clés</a> .
<b>service de répllication Exchange</b>	<i>(terme propre à Microsoft Exchange Server)</i> Service Microsoft Exchange Server qui représente les groupes de stockage répliqués au moyen de la technologie LCR (Local Continuous Replication) ou CCR (Cluster Continuous Replication). Voir aussi <a href="#">Cluster Continuous Replication</a> et <a href="#">Local Continuous Replication</a> .
<b>services Terminal Server</b>	<i>(terme propre à Windows)</i> 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.
<b>session</b>	Voir <a href="#">session de sauvegarde</a> , <a href="#">session de gestion de supports</a> et <a href="#">session de restauration</a> .
<b>session de consolidation d'objet</b>	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.
<b>session de copie d'objet</b>	Processus créant une copie supplémentaire des données sauvegardées sur un jeu de supports différent. Au cours de la session, les objets sauvegardés sélectionnés sont copiés du support source vers le support cible.
<b>session de gestion de supports</b>	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.
<b>session de restauration</b>	Processus permettant de copier les données de supports de sauvegarde vers un client.
<b>session de sauvegarde</b>	Processus consistant à créer une copie des données sur un support de stockage. Les activités sont définies dans une spécification de sauvegarde ou dans une session interactive. Tous les clients configurés dans une spécification de sauvegarde sont sauvegardés ensemble lors d'une session de sauvegarde

unique, avec le même type de sauvegarde. Une session de sauvegarde génère un jeu de supports sur lesquels des données ont été écrites, également appelé "jeu de sauvegarde" ou "jeu de supports".

Voir aussi [spécification de sauvegarde](#), [sauvegarde complète](#) et [sauvegarde incrémentale](#).

<b>session de vérification d'objet</b>	Processus qui vérifie l'intégrité des données d'objets sauvegarde ou de versions d'objets spécifiés ainsi que la capacité de sélectionner ou non des composants de réseau Data Protector pour les fournir à un hôte spécifié. Les sessions de vérification d'objet peuvent être exécutées de façon interactive ou conformément à des spécifications automatiques, planifiées ou de post-sauvegarde.
<b>SGBDR</b>	Système de gestion de base de données relationnelle.
<b>SIBF</b>	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.
<b>simultanéité</b>	Voir <a href="#">Agents de disque simultanés</a>
<b>SMBF</b>	Les fichiers binaires de messages de session (SMBF), un élément de l'IDB (base de données interne), contiennent les messages générés lors des sessions de sauvegarde, de restauration, de copie d'objet, de consolidation d'objet, de vérification d'objet et de gestion des supports. Chaque session génère un fichier binaire. Les fichiers sont regroupés par année et par mois.
<b>snapshot</b>	<i>(terme propre à HP P6000 EVA Array Family, à HP P9000 XP Array Family et à HP StorageWorks P4000 SAN Solutions)</i> Type de volume cible créé à l'aide d'une technologie de réplication spécifique. Selon le modèle de baie de disques et la technique de réplication choisie, différents types de snapshot avec des caractéristiques variées sont disponibles. Chaque snapshot peut être soit une copie virtuelle, qui dépend encore du contenu du volume source, soit une copie indépendante (clone) du volume source. Voir aussi <a href="#">réplique</a> et <a href="#">création de snapshot</a> .

<b>snapshot transportable</b>	<i>(terme propre à Microsoft VSS)</i> Copie miroir créée sur le système d'application et pouvant être présentée au système de sauvegarde où est effectuée une sauvegarde. Voir aussi <a href="#">Microsoft Volume Shadow Copy Service (VSS)</a> .
<b>spécification de sauvegarde</b>	Liste d'objets à sauvegarder avec un ensemble de périphériques ou de lecteurs à utiliser, des options de sauvegarde pour tous les objets de la spécification, et la date et l'heure d'exécution des sauvegardes. 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.
<b>Split Mirror</b>	<i>(terme propre aux baies de disques EMC Symmetrix et à HP P9000 XP Array Family)</i> Type de volume cible créé à l'aide d'une technologie de réplication spécifique. Une réplique Split Mirror fournit des copies indépendantes (clones) des volumes sources. Voir aussi <a href="#">réplique</a> et <a href="#">création de split mirror</a> .
<b>SRDF</b>	<i>(terme propre à EMC Symmetrix)</i> 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.
<b>stratégie d'allocation de supports</b>	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.
<b>stratégie d'utilisation des supports</b>	La stratégie d'utilisation des supports permet de contrôler la manière dont les nouvelles sauvegardes sont ajoutées aux supports déjà utilisés. Les options sont les suivantes : Ajout possible, Sans possibilité d'ajout et Ajout possible aux incrémentales uniquement.

**SYMA (terme propre à EMC Symmetrix)**

Voir [Agent EMC Symmetrix](#).

**système cible**

(terme propre à la récupération après sinistre) Système ayant subi un incident informatique. 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. Contrairement au cas d'un système défaillant, tout le matériel défectueux d'un système cible est remplacé.

**système d'application**

(terme propre à la sauvegarde ZDB) Système sur lequel s'exécute 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](#).

**système d'exploitation de récupération après sinistre**

Voir [DR OS](#).

**système d'hébergement**

Client Data Protector en fonctionnement utilisé pour la récupération après sinistre avec restitution de disque à l'aide d'un Agent de disque Data Protector installé.

**système d'origine**

Configuration système sauvegardée par Data Protector avant qu'un sinistre ne frappe le système.

**Système de bibliothèques virtuelles (VLS)**

Périphérique de stockage de données sur disque hébergeant une ou plusieurs bibliothèques de bandes virtuelles (VTL).

**système de fichiers**

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.

**Système de fichiers distribués (DFS)**

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.

**système de sauvegarde**

(terme propre à la sauvegarde ZDB) Système connecté à une baie de disques avec un ou plusieurs systèmes d'application. Le système de sauvegarde est généralement connecté à une



baie de disques pour créer des volumes cibles (une réplique) et sert à monter les volumes cibles (la réplique).  
Voir aussi [système d'application](#), [volume cible](#) et [réplique](#).

<b>SysVol</b>	<i>(terme propre à Windows)</i> Répertoire partagé contenant la copie des fichiers publics du domaine sur le serveur. Ces fichiers sont reproduits sur tous les contrôleurs du domaine.
<b>table des journaux de transactions</b>	<i>(terme propre à Sybase)</i> Table système où sont enregistrées automatiquement toutes les modifications apportées à la base de données.
<b>thread</b>	<i>(terme propre à Microsoft SQL Server)</i> Entité exécutable appartenant à un seul processus. Elle comprend un compteur de programme, une pile en mode utilisateur, une pile en mode noyau et un ensemble de valeurs de registre. Plusieurs threads peuvent être exécutés en même temps dans un même processus.
<b>TimeFinder</b>	<i>(terme propre à EMC Symmetrix)</i> Processus Business Continuanace permettant de créer une copie instantanée d'un ou de 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.
<b>TLU</b>	Tape Library Unit ou unité de bibliothèque de bandes.
<b>TNSNAMES.ORA</b>	<i>(terme propre à Oracle et SAP R/3)</i> Fichier de configuration réseau contenant des descripteurs de connexion mappés à des noms de services. Le fichier peut être géré au niveau central ou au niveau local afin d'être accessible à tous les clients ou à certains d'entre eux seulement.
<b>transaction</b>	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.
<b>type de support</b>	Type physique d'un support, comme DDS ou DLT.
<b>types de sauvegarde</b>	Voir <a href="#">sauvegarde incrémentale</a> , <a href="#">sauvegarde différentielle</a> , <a href="#">sauvegarde de transaction</a> , <a href="#">sauvegarde complète</a> et <a href="#">sauvegarde delta</a> .

<b>UIProxy</b>	Le serveur d'interface utilisateur graphique Java (le service <code>UIProxy</code> ) 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.
<b>unité de commande principale (MCU, pour Main Control Unit)</b>	<i>(terme propre à HP P9000 XP Array Family)</i> Unité HP StorageWorks P9000 XP Disk Array Family qui contient les volumes principaux (P-VOL) pour la configuration HP CA P9000 XP ou HP CA+BC P9000 XP et agit comme un périphérique maître. <i>Voir aussi <a href="#">HP Business Copy (BC) P9000 XP</a>, <a href="#">HP Continuous Access (CA) P9000 XP</a> et <a href="#">LDEV</a>.</i>
<b>Unité de télécommande (RCU)</b>	<i>(terme propre à HP P9000 XP Array Family)</i> Unité HP StorageWorks P9000 XP Disk Array Family qui sert de dispositif esclave pour l'unité de commande principale (MCU) dans la configuration HP CA P9000 XP ou HP CA + BC P9000 XP. Dans les configurations bidirectionnelles, la RCU peut également agir comme une MCU.
<b>User Account Control (UAC)</b>	Contrôle des comptes utilisateur - Composant de sécurité des systèmes d'exploitation Windows Vista, Windows 7 et Windows Server 2008 qui limite les logiciels d'application aux privilèges utilisateurs standard jusqu'à ce qu'un administrateur autorise une augmentation du niveau de privilèges.
<b>vérification</b>	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.
<b>vérification d'objet</b>	Processus consistant à vérifier l'intégrité des objets sauvegarde, du point de vue de Data Protector, et aptitude de Data Protector à les transmettre à la destination souhaitée. Ce processus peut servir à fournir un niveau de confiance en matière de capacité à restaurer des versions d'objets créées par des sessions de sauvegarde, de copie d'objet ou de consolidation d'objet.
<b>version de fichier</b>	Un même fichier peut être sauvegardé plusieurs fois lors de 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.

<b>Virtual Controller Software (VCS)</b>	<i>(terme propre à HP P6000 EVA Array Family)</i> Micrologiciel gérant tous les aspects du fonctionnement du système de stockage, dont les communications avec HP StorageWorks Command View EVA via les contrôleurs HSY. <i>Voir aussi <a href="#">HP StorageWorks Command View (CV) EVA</a>.</i>
<b>volser</b>	<i>(terme propre à ADIC et STK)</i> Un volser (VOLume SERIAL number - numéro de série de volume) est une étiquette située sur le support et servant à identifier la bande physique dans les très grandes bibliothèques. Il s'agit d'une appellation spécifique aux périphériques ADIC/GRAU et StorageTek.
<b>volume cible</b>	<i>(terme propre à la sauvegarde ZDB)</i> Volume de stockage sur lequel les données sont répliquées.
<b>volume de stockage</b>	<i>(terme propre à la sauvegarde ZDB)</i> Objet pouvant être présenté à un système d'exploitation ou à une autre entité (par exemple, un système de virtualisation) sur lequel existent des systèmes de gestion de volumes, 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.
<b>volume principal (P-VOL)</b>	<i>(terme propre à HP P9000 XP Array Family)</i> Disque interne (LDEV) d'une baie de disques HP StorageWorks P9000 XP Disk Array Family pour lequel il existe un volume secondaire (S-VOL) : son miroir ou un volume à utiliser pour le stockage des snapshots. Dans les configurations HP CA P9000 XP et HP CA + BC P9000 XP, les volumes principaux sont situés dans l'unité de commande principale (MCU). <i>Voir aussi <a href="#">volume secondaire (S-VOL)</a> et <a href="#">unité de commande principale (MCU)</a>.</i>
<b>volume secondaire (S-VOL)</b>	<i>(terme propre à HP P9000 XP Array Family)</i> Disque interne (LDEV) d'une baie de disques HP StorageWorks P9000 XP Disk Array Family qui est apparié à un autre LDEV : un volume principal (P-VOL). Il peut servir de miroir du P-VOL ou de volume

à utiliser pour le stockage des snapshots du P-VOL. Une adresse SCSI différente de celle utilisée pour le P-VOL est affectée au S-VOL. Dans une configuration HP CA P9000 XP, les S-VOL qui servent de miroirs peuvent être utilisés comme périphériques de secours dans une configuration MetroCluster.  
*Voir aussi [volume principal \(P-VOL\)](#) et [unité de commande principale \(MCU\)](#).*

<b>Volume Shadow Copy Service</b>	<i>Voir <a href="#">Microsoft Volume Shadow Copy Service (VSS)</a>.</i>
<b>volume source</b>	<i>(terme propre à la sauvegarde ZDB)</i> Volume de stockage contenant les données à répliquer.
<b>volume/disque/partition d'amorçage</b>	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.
<b>volume/disque/partition système</b>	Volume/disque/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.
<b>VSS</b>	<i>Voir <a href="#">Microsoft Volume Shadow Copy Service (VSS)</a>.</i>
<b>VxFS</b>	Veritas Journal Filesystem, système de fichiers journaux Veritas.
<b>VxVM (Veritas Volume Manager)</b>	Le VVM (Veritas Volume Manager), ou 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.
<b>Wake ONLAN</b>	Support de mise en marche distant pour les systèmes s'exécutant en mode d'économie d'énergie à partir d'un autre système du même réseau local.
<b>ZDB</b>	<i>Voir <a href="#">sauvegarde avec temps d'indisponibilité nul (ZDB)</a>.</i>
<b>zone de récupération flash</b>	<i>(terme propre à Oracle)</i> Groupe de disques de gestion de stockage automatique, de système de fichiers ou de répertoires gérés par Oracle qui sert de zone de stockage centralisé pour

des fichiers liés à la sauvegarde, la restauration et la récupération de base de données (fichiers de récupération).  
*Voir aussi [fichiers de récupération](#).*



---

# Index

## A

- accès à la bibliothèque
  - direct, 197
- accès direct à la bibliothèque, 197
- accès indirect à la bibliothèque, 197
  - accès à la bibliothèque, 196
- ADIC (EMASS/GRAU) AML, 180
- admin, groupe d'utilisateurs, 203
- Agent de support NDMP, 183
- Agent général de support, 183
- Agents d'application, 41
- Agents de disque, 41
- Agents de disque simultanés, 174, 332, 353
- Agents de sauvegarde, 41
- Agents de support, 41
  - Agent de support NDMP, 183
  - Agent général de support, 183
- ajout de données aux supports pendant une sauvegarde, 163
- ANSI X3.27, étiquettes, 161
- Application Response Measurement, 229, 230
  - temps de réponse, 230
  - transactions, 230
- applications de gestion des services, 228
  - HP Performance Agent, 228
- après sauvegarde, copie d'objet, 124
- après sauvegarde, copie de supports, 134
- architecture
  - cellules, 39
  - gestionnaires de cellules, 39
  - périphériques de sauvegarde, 39
- architecture de base de données, 207
- architecture de Data Protector
  - cellule, 39
  - description logique, 40
  - description physique, 40
  - gestionnaires de cellules, 39
  - périphériques, 39
  - systèmes client, 39
- architecture de la base de données IDB, 207
  - base de données catalogue, 210
  - base de données de gestion des supports, 209
  - éléments de la base de données IDB, 208
  - fichiers binaires d'intégrations sans serveur, 213
  - fichiers binaires de catalogue des détails, 211
  - fichiers binaires de messages de session, 212
  - schéma des éléments de la base de données IDB, 209
- ARM 2.0, 230
- audit, 229
- autres méthodes de récupération après sinistre, 145
  - fournisseurs de systèmes d'exploitation, 146
  - outils tiers, 146

- avantages
  - sauvegarde sur disque, 270
  - sauvegarde synthétique, 276
  - Volume Shadow Copy Service, 311
- avantages de l'intégration en ligne, 266
- avantages de la base de données IDB, 206

## B

- Backup Session Manager (gestionnaire de session de sauvegarde), 240
- basculement, 87, 88
- base de données
  - architecture, 207
  - avantages, 206
  - base de données catalogue, 210
  - base de données de gestion des supports, 209
  - croissance et performances, 219
  - dans le Gestionnaire de celluleWindows, 206
  - dans un environnement Manager-of-Managers, 207
  - Fichiers binaires d'intégrations sans serveur, 213
  - fichiers binaires de catalogue des détails, 211
  - fichiers binaires de messages de session, 212
  - fonctionnement, 215
  - gestion de la base de données IDB, 218
  - gestionnaires de cellules UNIX, 207
  - protection de catalogue, 206
  - taille et croissance, 206

- base de données catalogue, 210
  - emplacement, 211
  - enregistrements, 210
  - journaliser seulement les noms de répertoire, 108
  - journaliser toutes les informations détaillées, 108
  - ne journaliser aucun détail, 108
  - niveau de journalisation des informations, 112
  - taille et croissance des enregistrements CDB autres que les noms de fichier, 211
  - taille et croissance des noms de fichier, 210
- base de données dans le Gestionnaire de cellule UNIX
  - emplacement IDB, 207
- base de données dans le Gestionnaire de cellule Windows, 206
  - emplacement IDB, 206
  - format IDB, 207
- base de données dans les gestionnaires de cellules UNIX
  - format IDB, 207
- base de données dans un environnement MoM, 207
  - base de données de gestion centralisée des supports, 207
- base de données de gestion centralisée des supports, 47, 207, 341
- base de données de gestion des supports, 209
  - emplacement, 209
  - enregistrements, 209
  - taille et croissance, 209
- base de données IDB dans un environnement MoM
  - base de données de gestion centralisée des supports, 207
- base de données interne
  - Voir IDB



- base de données, estimation de la taille, 226
- bases de données, 261
  - base de données de gestion centralisée des supports, 47
  - dbspaces, 261
  - espaces de table, 261
  - fichiers, 261
  - fichiers de contrôle, 262
  - fichiers de données, 262
  - interfaces de sauvegarde, 264
  - journaux de transactions, 262
  - mémoire cache, 263
  - points de contrôle, 263
  - sauvegardes en ligne, 264
  - segments, 261
  - tables, 261
- besoins relatifs à une stratégie de sauvegarde, 322, 337
- bibliothèque de base de données, 265
- bibliothèques, 47
  - bibliothèques HP StorageWorks DLT 4115w, 328
  - bibliothèques HP StorageWorks DLT 4228w, 346
  - chargeurs automatiques HP StorageWorks DAT, 347
  - chargeurs automatiques HP StorageWorks DAT24, 328
  - connexion à plusieurs systèmes, 183
  - console de gestion, prise en charge, 171
  - emplacements, 180
  - gestion des supports, 180
  - insertion et éjection des logements de bande, 181
  - lecteurs, 183
  - logements multiples, 181
  - partage, 181, 183
  - plage d'emplacements, 180
  - prise en charge des bandes nettoyantes, 182
  - prise en charge des codes-barres, 181
  - silo, 180
  - taille, 180
- bibliothèques de bandes magnéto-optiques, 179
  - Voir aussi* bibliothèques
- bibliothèques HP StorageWorks DLT 4115w, 328
- bibliothèques HP StorageWorks DLT 4228w, 346
- bibliothèques, partage, 181, 183
- boucle, topologie, 191
- BSM, 240

## C

- caractéristiques de Data Protector, 33
- CDB
  - Voir* base de données catalogue
- Cell Request Server, 238

- cellules
  - description logique, 40
  - description physique, 40
  - distantes, 68
  - domaines Windows, 66
  - environnement mixte, 67
  - environnement UNIX, 66
  - environnement Windows, 66
  - gestion centralisée, 46
  - gestionnaires de cellules, 40
  - groupes de travail Windows, 67
  - multiples, 45, 63
  - opération de restauration, 41
  - opération de sauvegarde, 41
  - planification, 63
  - planification de la sécurité, 76
  - séparation, 45
- cellules distantes, 68
- cellules distantes géographiquement, 68
- cellules multiples, 45, 63
- chaînage de périphériques, 173
- chaîne de restauration, 104
- chaînes de périphériques, 178, 179
- chargeurs automatiques, 179
  - Voir aussi bibliothèques*
- chargeurs automatiques HP StorageWorks DAT24, 328, 347
- clé de cryptage
  - serveur gestionnaire de clés, 79
- client d'application
  - sauvegarde de snapshot, 297
  - Split Mirror, sauvegarde, 284
- client d'interface Java, 54
- client de sauvegarde
  - sauvegarde de snapshot, 297
  - Split Mirror, sauvegarde, 285
- client de sauvegarde comme serveur de basculement
  - sauvegarde de snapshot, 305
  - Split Mirror, sauvegarde, 287
- clients, 41
  - installation, 65
  - maintenance, 65
- cluster (définition), 85
- CMMDB, 47, 207, 341
  - Voir base de données de gestion centralisée des supports*
- codage, 79
- codage des données, 79
- codes-barres, 181
- commandes
  - omniclus, commande, 96
  - post-exécution, 242, 263
  - pré-exécution, 242, 263
- commutée, topologie, 192
- comparaison
  - périphériques sur disque, 271
- compression
  - logicielle, 72
  - matériel, 72
  - matérielle, 70
- compression logicielle, 72
- compression matérielle, 70, 72
- comptes utilisateur Data Protector, 77
- concepts
  - sauvegarde de snapshot, 296
  - sauvegarde Split Mirror, 283
- concepts de Data Protector
  - cellules, 39
  - clients, 39
  - gestionnaires de cellules, 39
  - périphériques, 39
- concepts de gestion des supports, 48
- configuration de cellules, 325, 341
- configuration de Data Protector, 55
- configuration de Data Protector (présentation), 55
- configuration de l'environnement de sauvegarde
  - gestion de la base de données IDB, 218

- configuration de la base de données IDB
  - création d'une spécification de sauvegarde de la base de données IDB, 218
  - gestion de la base de données IDB, 218
- configuration de périphériques, 170
  - grandes bibliothèques, 179
  - magasins, 179
  - périphériques autonomes, 178
- configuration de sauvegarde, 114
- configuration de spécifications de sauvegarde, 111
- configurations de snapshot, 301
  - autres, 305
  - baie de disques simple - hôte double, 301
  - baies de disques - hôte simple, 305
  - baies de disques multiples - hôte double, 303
  - hôtes d'application multiples - hôte de sauvegarde simple, 304
- configurations split mirror, 287
  - autres configurations, 292
  - miroir distant, 289
  - miroir local - hôte double, 287
  - miroir local - hôte simple, 289
  - miroir local/distant, 291
- conflit, 177
- console de gestion
  - Voir* console de gestion de bibliothèque
- console de gestion de bibliothèque, prise en charge, 171
- consolidation d'une chaîne de restauration, 128
- contrôle, 36, 232
- contrôle des services, 231
- conventions
  - document, 29
- copie automatisée des supports, 134
  - exemples, 356
- copie d'objet planifiée, 124
- copie d'objets, 123
  - à des fins de mise au coffre, 127
  - mettre en œuvre la sauvegarde de disque en plusieurs étapes, 128
  - migrer vers un autre type de support, 128
  - pour démultiplexer un support, 127
  - pour libérer un support, 127
  - regrouper une chaîne de restauration, 128
- copie de données sauvegardées, 121
- copie de supports, 133
  - automatisée, 134
  - copie intelligente de supports, 135
- copie de supports planifiée, 134
- copie des supports intelligente automatisée, 135
- copie des supports intelligente interactive, 136
- copie intelligente de supports, 135
- copie miroir, 308
- copies de supports, 133
- création de cellules
  - domaines Windows, 66
  - environnement mixte, 67
  - environnement UNIX, 66
  - environnement Windows, 66
  - groupes de travail Windows, 67
- création de spécifications de sauvegarde, 111
- croissance de l'environnement de sauvegarde
  - facteurs clés des performances et de la croissance de la base de données, 220

- croissance et performances de la base de données IDB, 219
  - base de données, estimation de la taille, 226
  - facteurs clés, 219
  - paramètres clés réglables, 220
  - sauvegardes comme facteurs clés, 220
- croissance et performances de la base, paramètres clés réglables, 220, 221
  - niveau de journalisation, 221
  - protection de catalogue, 223
  - utilisation du niveau de journalisation et de la protection de catalogue, 224
- CRS, 238
- cryptage, 79
  - clé de cryptage, 79
  - communications de contrôle cryptées, 82, 84
  - emplacement de la banque de clés, 214
  - emplacement du fichier catalogue, 214
  - répertoire d'exportation de clés, 217
  - serveur gestionnaire de clés, 80
  - sur disque, 79, 81
  - sur logiciel, 80
- cryptage des données, 79
- cycle de vie, supports, 149

## D

- dbspaces, 261
- DCBF
  - Voir* fichiers binaires de catalogue des détails
- DCBF, taille et croissance
  - fichiers binaires de catalogue des détails, 211

- définition de la protection de catalogue
  - utilisation du niveau de journalisation et de la protection de catalogue, 224
- délai d'attente, 243
- délai d'attente (sessions de restauration), 246
- demandes de montage, 243, 252, 255
  - automatisation, 244
  - notification, 244
  - réponse, 244, 247
- demandes de montage (sessions de restauration), 247
- démultiplexage d'un support, 127
- détection d'une bande nettoyante, 181
- détection de disques (définition), 244
- détection de lecteur encrassé, 182
- diffusions, 229
- disques partagés, 86
- distribution des objets sur les supports, 73
- document
  - conventions, 29
  - documentation connexe, 21
- document de métadonnées de module d'écriture (WMD), 313
- documentation
  - commentaires, 31
  - site Web de HP, 21
- documentation connexe, 21
- domaines Windows, 66
- données
  - masquer aux autres utilisateurs, 78
  - visibilité, 78
- données sauvegardées
  - masquer aux autres utilisateurs, 78
  - visibilité, 78
- données SIBF
  - fichiers binaires d'intégrations sans serveur, 213
- droits utilisateur, 202, 204
- droits utilisateur Data Protector (définition), 78

- duplication de données sauvegardées, 121
- durée d'une sauvegarde
  - exemples de calculs, 329, 348
- durée de la restauration, 138
  - facteurs ayant une influence, 139
  - restauration parallèle, 139
- durée de stockage des données sauvegardées, 106 - 109

## E

- e-mail, 229
- état des supports, 166
  - bon, 163
  - détermination, 166
  - médiocre, 163
  - passable, 163
- éléments de la base de données IDB
  - architecture, 208
- étiquetage des supports, 161
- étiquettes, 161
- échangeurs, 179
  - Voir aussi* bibliothèques
- EMC Symmetrix, 284
- emplacement d'un support, 160
- emplacement de la banque de clés cryptage, 214
- emplacement de la CDB
  - base de données catalogue, 211
- emplacement de la MMDB
  - base de données de gestion des supports, 209
- emplacement des DCBF
  - fichiers binaires de catalogue des détails, 212
- emplacement des SIBF
  - fichiers binaires d'intégrations sans serveur, 213
- emplacement des SMBF
  - fichiers binaires de messages de session, 213

- emplacement du fichier catalogue cryptage, 214
- emplacement IDB
  - Gestionnaire de cellule Windows, 206
  - gestionnaires de cellules UNIX, 207
- emplacements, 180
- emplacements, champs, 161
- en ligne, sauvegarde de base de données
  - sauvegarde de journaux d'archive, snapshot, 298
  - sauvegarde de journaux d'archive, Split Mirror, 285
  - sauvegarde de snapshot, 298
  - sauvegarde Split Mirror, 285
- enregistrements CDB
  - base de données catalogue, 210
- enregistrements MMDB
  - base de données de gestion des supports, 209
- enregistrements SMBF
  - fichiers binaires de messages de session, 212
- entreprise, stratégies de sauvegarde, 169
- environnement
  - entreprise, 44
  - Manager-of-Managers, 44
  - mixte, 67
  - réseau, 38
  - UNIX, 66
  - Windows, 66
- environnement d'entreprise, 44
- environnement mixte, 67
- environnements de sauvegarde, 319, 335
- espaces de table, 261

- exemples
  - génération de rapports et notification, [233](#)
  - mise au coffre, [169](#)
  - scénarios de sauvegarde, [317](#)
  - stratégies de planification, [117](#)
  - utilisation de pools de supports, [155](#)
  - utilisation des données fournies par Data Protector, [236](#)
- exemples d'utilisation de pools de supports, [155](#)
  - configuration de grande bibliothèque, [156](#)
  - périphériques multiples/pool unique, [157](#)
  - périphériques multiples/pools multiples, [158](#)
  - un périphérique/un pool, [155](#)
- exemples de gestion des services, [236](#)
- exemples de stratégies d'utilisation de supports, [164](#)
- expiration de la protection de catalogue, [223](#)
- exploration de fichiers, [108](#)
- exportation de supports, [109](#)
  - fonctionnement de la base de données IDB, [217](#)
  - objets supprimés, [217](#)
  - répertoire d'exportation de clés, [217](#)

## F

- facteurs ayant une influence sur la durée de la restauration, [139](#)
- facteurs clés des performances et de la croissance de la base de données, [219](#)
  - croissance de l'environnement de sauvegarde, [220](#)
  - variations du système de fichiers, [220](#)
- facteurs d'état des supports, [166](#)
- facteurs d'une stratégie de sauvegarde, [61](#)

- facteurs de croissance de la base de données catalogue
  - niveau de détails, [108](#)
  - protection de catalogue, [108](#)
- facteurs influant sur les stratégies de sauvegarde, [61](#)
- FC-AL, [191](#)
- Fibre Channel
  - planification des performances, [75](#)
- Fibre Channel (définition), [190](#)
- Fibre Channel Arbitrated Loop, [191](#)
- fichier binaire DC
  - fichiers binaires de catalogue des détails, [211](#)
  - fonctionnement de la base de données IDB, [215](#)
- fichier fnames.dat
  - taille et croissance des noms de fichier, [210](#)
- fichier individuel, restauration, [248](#)
- fichiers binaires d'intégrations sans serveur, [213](#)
  - données, [213](#)
  - emplacement, [213](#)
  - taille et croissance, [213](#)
- fichiers binaires de catalogue des détails, [211](#)
  - DCBF, taille et croissance, [211](#)
  - emplacement, [212](#)
  - fichier binaire DC, [211](#)
  - informations, [211](#)
  - répertoire DC, [212](#)
- fichiers binaires de messages de session, [212](#)
  - emplacement, [213](#)
  - enregistrements, [212](#)
  - taille et croissance, [212](#)
- fichiers de contrôle, [262](#)
- fichiers de données, [262](#)
- fonctionnalités de Data Protector, [33](#)
- fonctionnalités de sécurité, [76](#)
- fonctionnement d'une base de données, [261](#)

- fonctionnement de Data Protector, [237 - 259](#)
- fonctionnement de la base de données IDB, [215](#)
  - enregistrement d'emplacement de support, [215](#)
  - exportation de supports, [217](#)
  - fichier binaire DC, [215](#)
  - fichiers binaires de messages de session, [215](#)
  - maintenance quotidienne, [218](#)
  - purge de noms de fichier, [218](#)
  - restauration, [215](#)
  - sauvegarde, [215](#)
  - vérification, [216](#)
- format IDB
  - Gestionnaire de cellule Windows, [207](#)
  - gestionnaires de cellules UNIX, [207](#)
- formatage des supports, [149](#)
- fournisseur de copie miroir, [308](#)
- fragmentation, [74](#)
- fragmentation des disques, [74](#)

## G

- génération de rapports, [36](#), [232](#)
- génération de rapports et notification, [333](#), [353](#)
  - diffusions, [229](#)
  - e-mail, [229](#)
  - exemples, [233](#)
  - HTML, [229](#)
  - SNMP, [229](#)
- générations de sauvegarde, [160](#), [328](#), [347](#), [355](#)
- gestion centralisée des licences, [47](#)

- gestion de clusters, [85 - 97](#)
  - basculement, [87](#)
  - disponibilité du Gestionnaire de cellule, [88](#)
  - disques partagés, [86](#)
  - groupe, [87](#)
  - lecteurs flottants, [199](#)
  - MC/Service Guard, [86](#)
  - Microsoft Cluster Server, [86](#)
  - nœud principal, [87](#)
  - nœud secondaire, [87](#)
  - nœuds, [86](#)
  - package, [87](#)
  - partage de charge, [88](#)
  - périphériques, partage, [198](#)
  - pulsation, [87](#)
  - redémarrage automatique, [88](#)
  - sauvegarde des nœuds de cluster virtuels, [90](#), [92](#), [95](#)
  - serveur virtuel, [87](#)
  - Veritas Cluster, [86](#)
- gestion de la base de données IDB
  - configuration de l'environnement de sauvegarde, [218](#)
  - configuration de la base de données IDB, [218](#)
  - maintenance de la base de données IDB, [219](#)
  - présentation, [218](#)
  - récupération de la base de données IDB, [219](#)
- gestion des noms de fichier, [366](#)
- gestion des services, [36](#), [227 - 236](#)
  - analyses fonctionnelles de l'évolution des performances, [228](#)
  - Application Response Measurement, [229](#)
  - génération de rapports, [232](#)
  - moniteur, [232](#)
  - notification, [232](#)
  - présentation, [227](#)

gestion des supports, [48](#), [147 - 170](#), [180](#)

copie de supports, [133](#)

cycle de vie des supports, [149](#)

pools de supports, [48](#)

gestion des supports après la sauvegarde, [167](#)

gestion des supports avant la sauvegarde, [160](#)

gestion des supports pendant la sauvegarde, [162](#)

gestion des supports, session (définition), [258](#)

gestion informatique, [228](#)

Gestionnaires de cellule, [65](#)

gestionnaires de cellule

haute disponibilité, [88](#)

gestionnaires de cellules

optimisation de la charge, [243](#)

grandes bibliothèques, [179 - 188](#)

GRAU/EMASS, [179](#)

groupe, [87](#)

groupes d'utilisateurs, [202](#)

admin, [203](#)

opérateur, [203](#)

prédéfinis, [202](#), [203](#)

utilisateur final, [203](#)

Groupes d'utilisateurs Data Protector, [77](#)

groupes d'utilisateurs prédéfinis, [202](#), [203](#)

groupes de travail Windows, [67](#)

## H

haute disponibilité, [35](#), [88](#)

sauvegarde de snapshot, [295](#)

Split Mirror, sauvegarde, [285](#)

help (aide)

obtention, [31](#)

HP Performance Agent, [228](#), [230](#)

HP StorageWorks P4000 SAN Solutions, [296](#)

HP StorageWorks P6000 EVA Disk Array Family, [296](#)

HP StorageWorks P9000 XP Disk Array Family, [284](#)

HTML, [229](#)

## I

IDB, [205](#)

avantages, [206](#)

IDB (base de données interne)

architecture, [207](#)

base de données catalogue, [210](#)

base de données de gestion des supports, [209](#)

dans le Gestionnaire de cellule UNIX, [207](#)

dans le Gestionnaire de celluleWindows, [206](#)

dans un environnement

Manager-of-Managers, [207](#)

fichiers binaires d'intégrations sans serveur, [213](#)

fichiers binaires de catalogue des détails, [211](#)

fichiers binaires de messages de session, [212](#)

fonctionnement, [215](#)

gestion, [218](#)

taille et croissance, [206](#)

identification des supports, [181](#)

image disque ou système de fichiers, sauvegardes, [73](#)

image disque, sauvegardes, [73](#)

indirect

Storage Area Networks, [196](#)

Inet Data Protector, [238](#)

influence du niveau de journalisation et de la protection de catalogue sur la croissance de la base de données IDB, [221](#)

informations complémentaires, [355](#)

informations diverses, [355](#)



- Informations sur les DCBF
  - fichiers binaires de catalogue des détails, 211
- initialisation des supports, 149
  - ID de support, 160
- intégration aux applications de base de données en ligne, 37, 261 - 266
- intégration de cluster
  - présentation, 88
- intégrations, 231
  - Volume Shadow Copy Service, 312
- intégrations en ligne, 266
- interconnectivité, 189
- interface graphique Java de Data Protector, 52
- interface utilisateur graphique de Data Protector, 51
  - interface graphique Java de Data Protector, 52
- interfaces de sauvegarde, 264
- interfaces utilisateur, 41, 50
  - interface graphique Java de Data Protector, 52
  - interface utilisateur graphique de Data Protector, 51
- interfaces utilisateur de Data Protector, 41, 50
- internationalisation, 365

## J

- jeu de copies miroir, 308
- jeu de répliques
  - sauvegarde de snapshot, 299
  - Split Mirror, sauvegarde, 287
- jeu de supports
  - algorithme de sélection, 139
  - définition, 114
- jeux de codes, 367
- journaliser seulement les noms de répertoire
  - base de données catalogue, 108

- journaliser toutes les informations détaillées
  - base de données catalogue, 108
- journaux de transactions, 262

## K

- KMS, 80, 238
  - Voir serveur gestionnaire de clés

## L

- lecteurs, 196
  - connexion à plusieurs systèmes, 183
  - flottant, 199
  - statique, 198
- lecteurs flottants, 199
- lecteurs statiques, 198
- libération de supports, 127
- LIP, 191
- listes de périphériques, 172
- Localisation, 365
- logements multiples, 181
- logiciel HP Operations Manager, 229, 231
- Loop Initialization Primitive (protocole), 191

## M

- magasin, périphériques
  - nettoyage, 179
- maintenance de la base de données IDB
  - gestion de la base de données IDB, 219
- maintenance quotidienne
  - fonctionnement de la base de données IDB, 218
- Manager-of-Managers, 46, 47, 343
  - cellules distantes, 68
  - partage de bibliothèques, 47
  - rapports d'entreprise, 47

MC/Service Guard, 86  
Media Management Daemon (démon de gestion des supports), 238  
Media Session Managers (gestionnaires de session de gestion des supports), 258  
mémoire cache, 74, 263  
Microsoft Cluster Server, 86  
migration vers un autre type de support, 128  
mise au coffre, 149, 168 - 170, 333, 353  
    définition, 168  
    restauration, 169  
    restauration à partir d'un coffre, 334, 354  
mise au coffre, exemple, 169  
mise en attente  
    sessions de consolidation d'objet, 255  
    sessions de copie d'objet, 252  
    sessions de restauration, 246  
mise en miroir d'objets, 130  
mise hors service des supports, 149  
MMD, 238  
MMDB  
    Voir base de données de gestion des supports  
MMDB, taille et croissance  
    base de données de gestion des supports, 209  
modèle de sauvegarde VSS, 309  
module d'écriture, 308  
MoM, 46, 47  
MSM, 258

## N

ne journaliser aucun détail  
    base de données catalogue, 108

niveau de journalisation  
    activation de la restauration, 222  
    impact sur la capacité d'exploration pour la restauration, 222  
    impact sur la vitesse de l'IDB et les processus de sauvegarde, 222  
    impact sur la vitesse de restauration, 222  
    Journaliser fichiers, 221  
    Journaliser répertoires, 222  
    Journaliser tout, 221  
    Pas de journalisation, 222  
    taille et croissance de la base de données IDB, 206  
niveau de journalisation des informations, 112  
nombre de cellules, 63  
    éléments à prendre en considération, 63  
nombre de mémoires tampon, 176  
nombre de sessions simultanées  
    consolidation d'objet, 255  
    copie d'objet, 251  
    gestion des supports, 259  
    restauration, 246  
    sauvegarde, 241  
noms de verrouillage, 177, 195  
normes d'encodage des caractères, 366  
notification, 36  
nœud  
    cluster, 86  
    principal, 87  
    secondaire, 87  
nœud de cluster, 86  
nœud principal, 87  
nœud secondaire, 87  
nœuds de cluster virtuels, 90, 92, 95

## O

objet sauvegarde, 111  
objet, copie, 123

objets sauvegarde  
  vérification, 136  
objets, mise en miroir, 130  
omniclus, commande, 96  
opérateur, groupe d'utilisateurs, 203  
opération automatisée, 36, 119  
opération hors contrôle, 36, 119  
opération sans surveillance, 36, 119, 179  
optimisation de la charge sur le Gestionnaire de cellule, 243  
options de restauration, 332  
options de sauvegarde, 332, 352

## P

package, 87  
parallèle ou standard, restauration, 247  
parallélisme, 71  
partage de bibliothèques, 47, 180, 181, 183  
partage de charge, 71, 88, 112, 172  
partage de charge (définition), 172  
partage de périphériques dans un SAN, 193  
  lecteurs, 196  
  robot, 196  
performances des disques, 74  
  compression, 74  
  image disque, sauvegardes, 74  
  mémoire cache, 74  
périphérique de bibliothèque de fichiers, 272  
périphérique de bibliothèque de stockage de fichiers, 271  
périphérique de fichier autonome, 271  
périphérique en mode continu (définition), 173

périphériques, 49, 69, 170 - 199  
  ADIC (EMASS/GRAU) AML, 180  
  autonome, 178  
  bibliothèques de bandes magnéto-optiques, 179  
  bibliothèques HP StorageWorks DLT 4115w, 328  
  bibliothèques HP StorageWorks DLT 4228w, 346  
  bibliothèques SCSI, 179  
  chaînage de périphériques, 173  
  chargeurs automatiques, 179  
  chargeurs automatiques HP StorageWorks DAT, 347  
  chargeurs automatiques HP StorageWorks DAT24, 328  
  configuration, 170  
  console de gestion de bibliothèque, prise en charge, 171  
  échangeurs, 179  
  GRAU/EMASS, 179  
  listes de périphériques, 172  
  nombre de mémoires tampon, 176  
  noms de verrouillage, 177  
  partage de charge, 172  
  périphérique en mode continu, 173  
  périphériques multiples, 172  
  périphériques physiques, conflit, 177  
  planification des performances, 69  
  présentation, 170  
  prise en charge de TapeAlert, 171  
  prise en charge des bandes nettoyantes, 182  
  sélection pour une restauration, 140  
  simultanéité, 173  
  StorageTek/ACSLs, 179  
  sur disque, 271  
  taille de segment, 175  
  verrouillage de périphérique, 177  
périphériques autonomes, 178, 179  
périphériques chargeurs, 179  
périphériques de sauvegarde, 49, 69  
  présentation, 170

- périphériques multiples, 172
- périphériques physiques, conflit, 177
- périphériques sur disque
  - comparaison, 271
  - présentation, 269
- périphériques, configuration, 170
- périphériques, conflit, 177
- périphériques, partage dans les clusters, 198
- périphériques, partage dans un SAN, 193
  - lecteurs, 196
  - robot, 196
- plage d'emplacements, 180
- planification
  - configuration de sauvegarde, 114
- planification d'une stratégie de sauvegarde, 57 - 146
  - cryptage des données, 79
  - définition, 58
  - définition des besoins, 58
  - disponibilité des données du système, 61
  - gestion des supports, 63
  - périphériques, configuration, 62
  - planification de sauvegardes, 62
  - protection de catalogue, 62
  - protection des données, 62
  - stratégies de sauvegarde, 61
  - types de données, 61
- planification de cellules, 63 - 68
  - gestionnaires de cellule, 65
  - nombre de cellules, 63
  - Serveur d'installation, 65
- planification de la sécurité, 76 - 80
  - cellules, 76
  - codage des données, 79
  - communications de contrôle cryptées, 82, 84
  - comptes utilisateur Data Protector, 77
  - Groupes d'utilisateurs Data Protector, 77
  - visibilité des données sauvegardées, 78
- planification des performances, 69 - 75
  - compression, 70, 74
  - compression logicielle, 72
  - compression matérielle, 72
  - Fibre Channel, 75
  - fragmentation des disques, 74
  - infrastructure, 69
  - mémoire cache, 74
  - parallélisme, 71
  - partage de charge, 71
  - performances des disques, 74
  - périphériques, 69
  - sauvegardes locales, 69
  - sauvegardes réseau, 69
  - types de sauvegarde, 72
- planification échelonnée de sauvegardes complètes, 116
- planification, conseils et pièges à éviter, 115
- point à point, topologie, 191
- points de contrôle, 263
- pool de supports, propriétés
  - ajout possible, 150
  - ajout possible aux incrémentales uniquement, 150
  - stratégie d'allocation de supports, 150

- pools de supports, 48, 49, 150, 330, 348
    - définition, 150
    - exemples d'utilisation, 151, 155
    - par défaut, 150
    - propriétés, 150
  - pools de supports par défaut, 150
  - post-exécution, commandes, 242, 263
  - pré-exécution et post-exécution, scripts, 242
  - pré-exécution, commandes, 242, 263
  - préparation d'un plan de stratégie de sauvegarde, 61
  - préparation des supports, 149
  - présentation
    - gestion de la base de données IDB, 218
    - recupération après sinistre, 143
    - restauration, 38
    - sauvegarde de snapshot, 295
    - sauvegarde Split Mirror, 283
    - sauvegarde synthétique, 275
    - Volume Shadow Copy Service, 308
  - présentation des restaurations, 38
  - présentation des sauvegardes, 37
  - présentation générale
    - sauvegarde, 37
  - prévention des conflits, 177
  - priorité des emplacements des supports, 140
  - prise en charge de TapeAlert, 171
  - prise en charge des bandes nettoyantes, 182
    - magasin, périphériques, 179
    - magasins, 179
  - prise en charge des codes-barres, 181
- processus, 237
  - Backup Session Manager (gestionnaire de session de sauvegarde), 240
  - restauration, 38
  - Restore Session Managers (gestionnaires de session de restauration), 245
  - sauvegardes, 37
- processus Data Protector, 237 - 259
  - Cell Request Server, 238
  - Inet Data Protector, 238
  - Media Management Daemon (démon de gestion des supports), 238
  - Raima Database Server (serveur de base de données Raima), 238
  - serveur gestionnaire de clés, 238
- processus de sauvegarde
  - destination, 37
  - source, 37
- propriété, 79
  - sessions de restauration, 79
  - sessions de sauvegarde, 79
- propriété des sauvegardes, 79
- propriétés de pools de supports, 150
- protection de catalogue, 107, 332
  - comme paramètre clé réglable de l'IDB, 223
  - expiration, 223
  - exploration de fichiers, 108
  - générations de sauvegarde, 356
  - impact sur les performances de la sauvegarde, 223
  - restauration des données lorsque la protection de catalogue arrive à expiration, 223
  - taille et croissance de la base de données IDB, 206
- protection de catalogue comme paramètre clé réglable de l'IDB, 223
- protection des données, 107, 332
- public, 21

- pulsation, 87
- pulsation du cluster, 87
- purge
  - noms de fichier, 218
  - versions de fichier, 218
- purge de noms de fichier
  - fonctionnement de la base de données IDB, 218
- purge de versions de fichier, 218

## R

### RAID

- sauvegarde de snapshot, 296
- Split Mirror, sauvegarde, 287

Raima Database Server (serveur de base de données Raima), 238

rappports d'entreprise, 47

rappports en ligne, 235

rappports Java, 235

rappports Java en ligne, 235

RDS, 238

récupération, 144

- récupération après sinistre, 144

récupération après sinistre, 144

- alternatives, 145
- autres méthodes, 145
- concepts, 143
- phase 0, 144
- phase 1, 144
- phase 2, 144
- phase 3, 144
- présentation, 143

récupération de la base de données IDB

- gestion de la base de données IDB, 219

recyclage des supports, 149

répertoire DC

- fichiers binaires de catalogue des détails, 212

réplique

- sauvegarde de snapshot, 296
- Split Mirror, sauvegarde, 283

- réseau, environnement, 38
- restauration à partir de supports stockés dans un coffre, 169
- restauration complète de système de fichiers, 334, 354
- restauration des données, 138 - 143
- restauration instantanée
  - sauvegarde de snapshot, 299
  - Split Mirror, sauvegarde, 285
- restaurations, 138, 245
  - configuration, 72
  - durée, 138
  - fonctionnement de la base de données IDB, 215
  - mise au coffre, 169
  - opérateurs, 141
  - optimisation, 116
  - parallèles, 247
  - priorité des emplacements des supports, 140
  - restauration complète de système de fichiers, 334, 354
  - restaurer par requête, 334, 354
  - sélection des périphériques, 140
  - sélection des supports, 139
  - utilisateurs finaux
    - utilisateur final, groupe d'utilisateurs, 142
  - Volume Shadow Copy Service, 313
- restaurations parallèles, 247
- restaurer par requête, 334, 354
- Restore Session Managers (gestionnaires de session de restauration), 245
- robot, 196
- rotation des jeux de répliques
  - sauvegarde de snapshot, 299
  - Split Mirror, sauvegarde, 287
- RSM, 245

## S

### SAN

Voir Storage Area Networks

### sauvegarde

fonctionnement de la base de données IDB, 215

sur disque, 269

### sauvegarde avec temps d'indisponibilité nul

sauvegarde de snapshot, 295

sauvegarde Split Mirror, 283

sauvegarde complète synthétique, 275

sauvegarde complète virtuelle, 277

sauvegarde de disque en plusieurs étapes, 128

sauvegarde de données, 110 - 119  
procédure, 110

sauvegarde de journaux d'archive

sauvegarde de snapshot, 298

Split Mirror, sauvegarde, 285

sauvegarde de snapshot, 295

client d'application, 297

client de sauvegarde, 297

client de sauvegarde comme serveur de basculement, 305

concepts, 296

configuration, autre, 305

configuration, baie de disques simple - hôte double, 301

configuration, baies de disques - hôte simple, 305

configuration, baies de disques multiples - hôte double, 303

configuration, hôtes d'application multiples - hôte de sauvegarde simple, 304

configurations, 301

en ligne, sauvegarde de base de données, 298

haute disponibilité, 295

jeu de répliques, 299

présentation, 295

RAID, 296

réplique, 296

restauration instantanée, 299

rotation des jeux de répliques, 299

sauvegarde de journaux d'archive, 298

sauvegarde ZDB sur bande, 298

sauvegarde ZDB sur disque, 298

sauvegarde ZDB sur disque + bande, 298

volume cible, 296

volume source, 296

sauvegarde en ligne de bases de données, 264

sauvegarde en mode détection de disques, 244

sauvegarde en mode détection de disques ou standard, 244

sauvegarde incrémentale avancée, 100

sauvegarde incrémentale classique, 99

- sauvegarde standard ou en mode détection de disques, 244
- sauvegarde sur disque, 269
  - avantages, 270
- sauvegarde synthétique, 275
  - avantages, 276
  - fonctionnement, 276
  - restauration, 278
  - utilisation d'espace de support, 278
- sauvegarde VSS, 312
- sauvegarde ZDB sur bande
  - sauvegarde de snapshot, 298
  - Split Mirror, sauvegarde, 286
- sauvegarde ZDB sur disque
  - sauvegarde de snapshot, 298
  - Split Mirror, sauvegarde, 286
- sauvegarde ZDB sur disque + bande
  - sauvegarde de snapshot, 298
  - sauvegarde Split Mirror, 286
- sauvegarde, performances, 174
- sauvegardes
  - ajout de données aux supports, 163
  - automatisées, 120
  - configuration, 72
  - hors contrôle, 120
  - image disque, 73
  - locales, 69
  - objets sauvegarde, 111
  - périphériques, 170
  - planification échelonnée, 116
  - planifiées, 114
  - réseau, 69
  - sans surveillance, 120
  - sauvegarde en mode détection de disques ou standard, 244
  - sauvegarde standard ou en mode détection de disques, 244
  - sessions, 115
  - spécifications de sauvegarde, 111
  - stratégies de planification, 114
  - système de fichiers, 73
- sauvegardes complètes, 72
  - planification échelonnée, 116
- sauvegardes complètes et incrémentales, 98 - 106
- sauvegardes d'image disque, 74
- sauvegardes incrémentales, 72
  - module fournisseur d'informations sur les modifications, 100
  - types, 101
- sauvegardes incrémentales de niveau 1, 331, 350
- sauvegardes incrémentales par niveau, 101
- sauvegardes indépendantes du réseau local, 193
- sauvegardes planifiées, 114
- sauvegardes simultanées, 174, 332, 353
- scénarios de sauvegarde (entreprise ABC), 335, 354
- scénarios de sauvegarde (entreprise XYZ), 319, 334
- schéma des éléments de la base de données IDB
  - architecture de la base de données IDB, 209
- scripts
  - post-exécution, 113
  - pré-exécution, 113
  - pré-exécution et post-exécution, 242
- scripts post-exécution, 113
- scripts pré-exécution, 113
- sécurité
  - codage des données, 201
  - définition, 76
  - groupes d'utilisateurs, 201
  - interdiction de l'accès aux données, 201
  - système relatif aux utilisateurs, 201
  - visibilité des données sauvegardées, 202
- sécurité des données, 113
- segments, 261
- sélection d'objets sauvegarde, 111



- sélection des supports utilisés pour la sauvegarde, 163
- serveur d'interface Java, 53
- serveur gestionnaire de clés, 80, 238
- serveur virtuel, 87
- serveurs d'installation, 41, 65
- serveurs de lecteurs, 41
- services, 237
- services Data Protector, 237 - 259
  - Cell Request Server, 238
  - Inet Data Protector, 238
  - Media Management Daemon (démon de gestion des supports), 238
  - Raima Database Server (serveur de base de données Raima), 238
  - serveur gestionnaire de clés, 238
- session de consolidation d'objet automatique, 253
- session de consolidation d'objet interactive, 253
- session de copie d'objet automatique, 249
- session de copie d'objet interactive, 249
- session de sauvegarde
  - définition, 113, 239
  - propriété, 79
- sessions
  - consolidation d'objet, 253
  - copie d'objet, 249
  - gestion des supports, 258
  - restauration, 43, 245
  - sauvegarde, 42, 239
  - vérification d'objet, 256
- sessions de consolidation d'objet, 253
  - demandes de montage, 255
  - mise en attente, 255
- sessions de copie d'objet, 249
  - demandes de montage, 252
  - mise en attente, 252
- sessions de restauration, 43, 79, 245 - 248
  - définition, 245
  - délai d'attente, 246
  - demandes de montage, 247
  - mise en attente, 246
- sessions de sauvegarde, 42, 110, 115, 239 - 244
  - configuration de sauvegarde, 114
  - délai d'attente, 243
  - demandes de montage, 243
  - interactives, 239
  - planifiées, 239
- sessions de sauvegarde interactives, 239
- sessions de sauvegarde planifiées, 239
- sessions de vérification d'objet, 256
- sessions de vérification d'objet automatique, 256
- sessions de vérification d'objet interactives, 256
- sessions simultanées
  - consolidation d'objet, 255
  - copie d'objet, 251
  - gestion des supports, 259
  - restauration, 246
  - sauvegarde, 241
- SIBF, taille et croissance
  - fichiers binaires d'intégrations sans serveur, 213
- silo, bibliothèques, 180
- simultanéité, 173, 174
- sinistre, 143
- Site Web
  - support technique, 31
- sites Web
  - guides des produits, 21
  - HP, 31
  - HP Subscriber's Choice for Business, 31
- SMBF
  - Voir fichiers binaires de messages de session

- SMBF, taille et croissance
  - fichiers binaires de messages de session, [212](#)
- snapclones, [301](#)
- snapshots
  - types, [300](#)
- snapshots avec préallocation d'espace disque, [300](#)
- snapshots sans préallocation d'espace disque, [300](#)
- SNMP, [229](#)
- solutions pour scénarios de sauvegarde, [323](#), [340](#)
- spécifications de sauvegarde, [49](#), [111](#), [331](#), [349](#)

- Split Mirror, sauvegarde
  - client d'application, [284](#)
  - client de sauvegarde, [285](#)
  - client de sauvegarde comme serveur de basculement, [287](#)
  - concepts, [283](#)
  - configuration, autre, [292](#)
  - configuration, miroir distant, [289](#)
  - configuration, miroir local - hôte double, [287](#)
  - configuration, miroir local - hôte simple, [289](#)
  - configuration, miroir local/distant, [291](#)
  - configurations, [287](#)
  - en ligne, sauvegarde de base de données, [285](#)
  - haute disponibilité, [285](#)
  - jeu de répliques, [287](#)
  - présentation, [283](#)
  - RAID, [287](#)
  - réplique, [283](#)
  - restauration instantanée, [285](#)
  - rotation des jeux de répliques, [287](#)
  - sauvegarde de journaux d'archive, [285](#)
  - sauvegarde ZDB sur bande, [286](#)
  - sauvegarde ZDB sur disque, [286](#)
  - sauvegarde ZDB sur disque + bande, [286](#)
  - volume cible, [284](#)
  - volume source, [283](#)
- standard ou parallèle, restauration, [247](#)

- Storage Area Networks, 189 - 199
  - accès direct à la bibliothèque, 197
  - accès indirect à la bibliothèque, 196
  - concepts, 189
  - Fibre Channel, 190
  - interconnectivité, 189
  - noms de verrouillage, 195
  - partage de périphériques, 193
  - périphériques, partage, 193
  - périphériques, partage dans les clusters, 198
  - sauvegardes indépendantes du réseau local, 193, 195
  - topologies Fibre Channel, 191
- StorageTek/ACSLs, 179
- stratégie de rotation des supports (définition), 158
- stratégie de sauvegarde, 57
- stratégies d'allocation de supports, 150, 159, 163
  - souple, 163
  - stricte, 163
- stratégies d'utilisation de supports, 163
  - ajout possible, 164
  - ajout possible aux incrémentales uniquement, 164
  - exemples, 164
  - sans possibilité d'ajout, 164
- stratégies de planification, 114, 116
- stratégies de planification, exemples, 117
- stratégies de restauration, 138
  - opérateurs, 141
  - utilisateurs finaux, 142
- stratégies de rotation des supports, 158
- stratégies de sauvegarde, 44, 169
  - environnement d'entreprise, 44
- Subscriber's Choice, HP, 31
- support
  - âge, 167
  - codes-barres, 181
  - copie, 133
  - copie automatisée, 134
  - copie des supports intelligente avec VLS, 135
  - cryptage, 81
  - emplacements, champs, 161
  - erreurs de périphérique, 167
  - estimation de la quantité de supports requis, 159
  - étiquetage, 161, 181
  - exportation, 109
  - formatage, 149
  - initialisation, 149, 160
  - logements de bande, 181
  - logements de bande, éjection, 181
  - logements de bande, insertion, 181
  - marques de fichier, 175
  - mise au coffre, 149, 168
  - mise hors service, 149
  - nombre d'écrasements, 167
  - prise en charge des bandes nettoyantes, 182
  - prise en charge des codes-barres, 181
  - segments d'en-tête, 175
  - segments de catalogue, 175
  - segments de données, 175
  - sélection pour la sauvegarde, 163
  - sélection pour une restauration, 139
- support technique
  - HP, 31
  - localisateur de services, site Web, 31
- supports
  - distribution des objets, 73
  - préparation, 149
- supports de sauvegarde
  - vérification, 136
- supports, cycle de vie, 149
- supports, description, 160

- supports, fonctionnalité de gestion, 48, 147
- supports, gestion
  - ajout de données aux supports, 163
  - copies, 133
  - copies de supports, 133
  - état des supports, 163
  - étiquetage des supports, 161
  - mise au coffre, 168
  - pools de supports, 150
  - sélection des supports, 163
  - stratégies d'allocation de supports, 163
  - stratégies de préallocation, 163
  - stratégies de rotation des supports, 158
- supports, mise au coffre, 149
- surveillance, 232
- système cible, 143
- système de fichiers ou image disque, sauvegardes, 73
- système de fichiers, sauvegarde, 73
  - Volume Shadow Copy Service, 311, 313
- système de sécurité relatif aux utilisateurs, 201
- systèmes à sauvegarder, 41
- systèmes client, 41
- systèmes dotés de périphériques de sauvegarde, 41

## T

- tâches de copie d'objet, 126
- taille
  - bibliothèques, 180
- taille de bibliothèque, 180
- taille de bloc
  - par défaut, 176
  - performances, 176
  - périphériques, 176
  - périphériques de sauvegarde, 176
- taille de bloc par défaut, 176

- taille de segment, 175
- taille et croissance de la base de données IDB, 206
  - niveau de journalisation, 206
  - protection de catalogue, 206
- taille et croissance des enregistrements CDB autres que les noms de fichier
  - base de données catalogue, 211
- taille et croissance des noms de fichier
  - base de données catalogue, 210
  - fichier fnames.dat, 210
- temps de réponse, 230
- topologies Fibre Channel, 191
  - boucle, topologie, 191
  - commutée, topologie, 192
  - point à point, 191
- traitement des invites de montage, 120
- transactions, 230
- types de protection
  - catalogue, 107
  - données, 107
- types de sauvegarde, 116
  - complète, 72, 98, 99
  - incrémentale, 72, 98, 99
  - planification des performances, 72
- types de sauvegardes incrémentales, 101
  - sauvegardes incrémentales avancées, 100
  - sauvegardes incrémentales classiques, 99
  - sauvegardes incrémentales par niveau, 101

## U

- utilisateur final, groupe d'utilisateurs, 203
- utilisateurs, 202
- utilisateurs et groupes d'utilisateurs, 201 - 204
- utilisation de supports, 149
- utilisation des pools de supports, 151

- utilisation du niveau de journalisation et de la protection de catalogue, [224](#)
- définition de la protection de catalogue, [224](#)
- particularités des grandes cellules, [225](#)
- particularités des petites cellules, [225](#)
- utilisation de différents niveaux de journalisation dans la même cellule, [224](#)

## V

- variations du système de fichiers
  - facteurs clés des performances et de la croissance de la base de données, [220](#)
- vérification
  - fonctionnement de la base de données IDB, [216](#)
- vérification d'objet
  - flux de session, [257](#)
- vérification des supports et des objets de sauvegarde, [136](#)
- Veritas Cluster, [86](#)
- verrouillage de périphérique, [177](#)
- virtualisation du stockage, [295](#)
- visibilité des données sauvegardées, [78](#), [202](#)
- volume cible
  - sauvegarde de snapshot, [296](#)
  - Split Mirror, sauvegarde, [284](#)

- Volume Shadow Copy Service (VSS)
  - avantages, [311](#)
  - copie miroir, [308](#)
  - fournisseur de copie miroir, [308](#)
  - intégration à Data Protector, [311](#)
  - jeu de copies miroir, [308](#)
  - modèle de sauvegarde, [309](#)
  - module d'écriture, [308](#)
  - présentation, [307](#)
  - restauration, [313](#)
  - sauvegarde, [312](#)
  - sauvegarde et restauration de système de fichiers, [313](#)
  - système de fichiers, sauvegarde, [311](#)
- volume source
  - sauvegarde de snapshot, [296](#)
  - Split Mirror, sauvegarde, [283](#)
- VSS
  - Voir Volume Shadow Copy Service

