Guide d'installation et de choix des licences HP OpenView Storage Data Protector

Date de publication : juillet 2006

Référence constructeur : B6960-96023

Version A.06.00

Informations légales

La société Hewlett-Packard ne fournit aucune garantie à propos de ce manuel, y compris, mais non exclusivement en ce qui concerne les garanties implicites de qualité marchande et d'adaptation pour une utilisation particulière. Hewlett-Packard n'est pas responsable des erreurs présentes dans ce manuel ni des dommages fortuits ou consécutifs résultant de la mise à disposition, des performances ou de l'utilisation de cette documentation.

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

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

UNIX® est une marque déposée de The Open Group.

La société Hewlett-Packard n'est pas responsable des erreurs techniques ou éditoriales ou des omissions figurant dans le présent document. Les informations sont fournies en l'état sans aucune garantie et peuvent être modifiées sans préavis. Les garanties relatives aux produits de la société Hewlett-Packard sont décrites dans les déclarations de garantie expresse accompagnant lesdits produits. Aucun élément du présent document ne saurait être considéré comme une garantie supplémentaire.

Sommaire

Sommaire

Sommaire

C. Annexe C

Index

Sommaire

Informations sur cette documentation

La version du manuel est indiquée par sa date de publication et sa référence. La date de publication sera différente pour chaque nouvelle édition imprimée. Toutefois, des modifications mineures effectuées lors d'une nouvelle impression pourraient ne pas changer la date de publication. La référence du manuel changera lors de modifications importantes du manuel.

Entre les différentes éditions des manuels, des mises à jour pourraient 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	Date de publication	Produit
B6960-90079	Mai 2003	Data Protector version A.05.10
B6960-90107	Octobre 2004	Data Protector version A.05.50
B6960-96023	Juillet 2006	Data Protector version A.06.00

Conventions typographiques

Dans ce manuel, les conventions typographiques suivantes seront utilisées :

Tableau 2

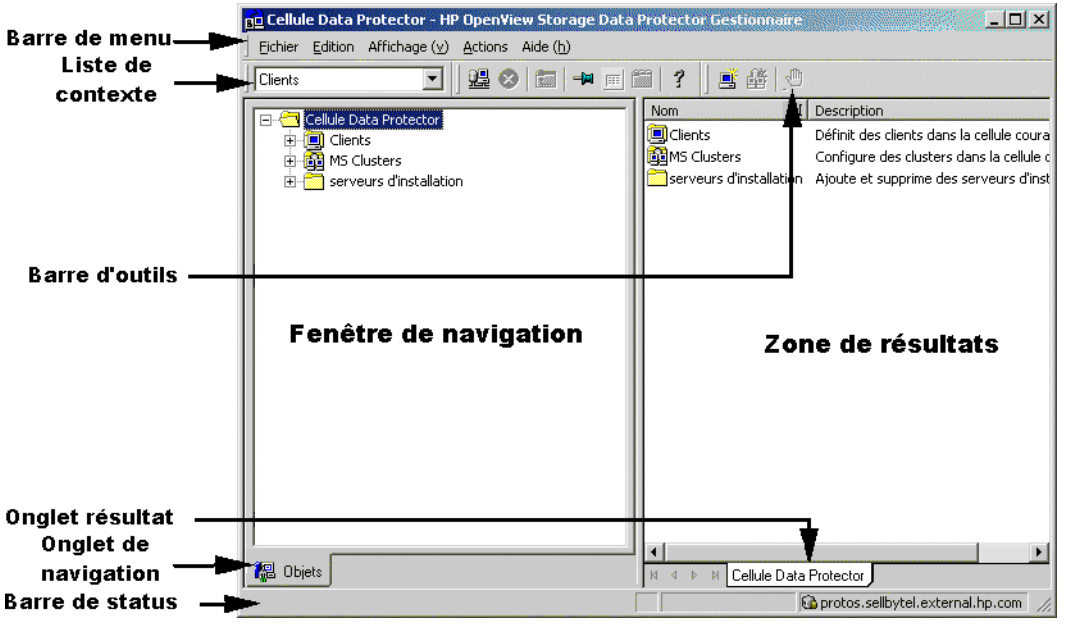
Convention	Signification	Exemple
Italiques	Titres de manuels ou d'autres documents, titres sur les différentes pages des manuels.	Pour plus d'informations, reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector*.
	Fait ressortir le texte.	Vous *devez* suivre la procédure décrite.
	Indique une variable que vous devez fournir lorsque vous entrez une commande.	A l'invite, entrez : `rlogin` *`votre_nom`* en remplaçant "votre_nom" par votre nom de connexion.
Gras	Termes nouveaux	Le **Gestionnaire de cellule** de Data Protector est l'élément principal...

Tableau 2

Convention	Signification	Exemple
`Système`	Texte et autres éléments apparaissant à l'écran	Le système affiche alors : `Appuyez sur Entrée`
	Noms de commande	Utilisez la commande `grep` pour ...
	Noms de fichier et de répertoire	`/usr/bin/X11`
	Noms de processus	Vérifiez que `Data Protector Inet` est en cours d'exécution.
	Noms de fenêtre et de boîte de dialogue	Dans la boîte de dialogue `Options de sauvegarde`, sélectionnez...
	Texte que vous devez saisir	A l'invite, entrez : `ls -l`
Touches du clavier	Touches du clavier	Appuyez sur **Entrée**.

L'interface graphique utilisateur de Data Protector se présente de la même façon sous Windows et UNIX. Pour en savoir plus sur l'interface graphique utilisateur de Data Protector, reportez-vous à l'aide en ligne.

Figure 1 Interface graphique utilisateur de Data Protector



Contacts

Informations générales

Vous trouverez des informations générales sur Data Protector à l'adresse suivante :

http://www.hp.com/go/dataprotector

Support technique

Vous trouverez des informations sur le support technique dans les centres de support électronique HP à l'adresse suivante :

http://www.itrc.hp.com

Vous trouverez des informations sur les correctifs Data Protector les plus récents à l'adresse suivante :

http://www.itrc.hp.com

HP ne fournit pas de support pour les logiciels et matériels tiers. Pour cela, contactez le fournisseur tiers.

Vos commentaires sur la documentation

Afin de mieux connaître vos besoins, nous vous remercions de bien vouloir nous faire part de vos commentaires concernant la documentation. Pour nous communiquer vos commentaires, utilisez l'adresse suivante :

storagedocs.feedback@hp.com

Formation

Pour obtenir des informations sur les formations HP OpenView proposées, consultez le site HP OpenView à l'adresse suivante :

http://www.openview.hp.com/training/

Suivez les liens pour obtenir des informations concernant les cours programmés, les formations sur site et les inscriptions aux cours.

Documentation Data Protector

La documentation de Data Protector se présente sous forme de manuels imprimés et d'aide en ligne.

Manuels

Les manuels Data Protector sont disponibles au format PDF et en version imprimée. Vous pouvez installer les fichiers PDF lors de l'installation de Data Protector en sélectionnant le composant `Interface utilisateur` sous Windows ou le composant `OB2-DOCS` sous UNIX. Les manuels sont alors placés dans le répertoire *<répertoire_Data_Protector>*`\docs` sous Windows ou `/opt/omni/doc/C/` sous UNIX. Vous pouvez également les consulter au format PDF à l'adresse suivante : http://www.hp.com/support/manuals

Guide conceptuel HP OpenView Storage Data Protector

Ce manuel décrit les concepts Data Protector et fournit des informations de fond sur le fonctionnement du logiciel. Il est conçu pour être utilisé avec l'aide en ligne du qui se concentre sur les tâches du logiciel.

Guide d'installation et de choix des licences HP OpenView Storage Data Protector

Ce manuel 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 OpenView Storage Data Protector

Enfin, il décrit comment résoudre les problèmes auxquels vous pouvez être confronté avec Data Protector.

Guide de récupération après sinistre HP OpenView Storage Data Protector

Vous y trouverez des instructions pour planifier, préparer et tester des procédures de reprise après sinistre.

Guide d'intégration HP OpenView Storage Data Protector

Ce manuel décrit la configuration et l'utilisation de Data Protector dans le cadre de la sauvegarde et de la restauration de différentes bases de données et applications. Il s'adresse aux opérateurs ou aux administrateurs de sauvegarde. Ce manuel existe en quatre versions :

- *Guide d'intégration HP OpenView Storage Data Protector pour les applications Microsoft : SQL Server, Exchange Server et Volume Shadow Copy Service*

  Ce manuel décrit les intégrations de Data Protector avec les applications Microsoft suivantes : Microsoft Exchange Server 2000/2003, Microsoft SQL Server 7/2000/2005 et Volume Shadow Copy Service.

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

  Ce manuel décrit les intégrations de Data Protector pour Oracle, SAP R3 et SAP DB.

- *Guide d'intégration HP OpenView Storage Data Protector pour les applications IBM : Informix, DB2 et Lotus Notes/Domino*

  Ce manuel décrit les intégrations de Data Protector avec les applications IBM suivantes : Informix Server, IBM DB2 et Lotus Notes/Domino Server.

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

  Ce manuel décrit les intégrations de Data Protector avec Sybase, Network Node Manager, Network Data Management Protocol et VMware.

Guide d'intégration HP OpenView Storage Data Protector pour HP OpenView

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

Guide d'intégration HP OpenView Storage Data Protector pour HP OpenView Operations pour UNIX

Ce manuel décrit la procédure de surveillance et de gestion de l'état et des performances de l'environnement Data Protector avec HP OpenView Operations (OVO), HP OpenView Service Navigator et HP OpenView Performance (OVP) sous UNIX.

Guide d'intégration HP OpenView Storage Data Protector pour HP OpenView Operations pour Windows

Ce manuel décrit la procédure de surveillance et de gestion de l'état et des performances de l'environnement Data Protector avec HP OpenView Operations (OVO), HP OpenView Service Navigator et HP OpenView Performance (OVP) sous Windows.

Ce manuel existe en deux versions :

- pour OVO 7.1x, 7.2x
- pour OVO 7.5

Guide conceptuel HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul

Ce manuel décrit les concepts Data Protector de sauvegarde avec temps d'indisponibilité nul et de restauration instantanée et fournit des informations de base sur le fonctionnement de Data Protector dans un environnement de sauvegarde avec temps d'indisponibilité nul. Il est destiné à être utilisé avec le *Guide de l'administrateur HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*, lequel met l'accent sur les tâches du logiciel, et avec le *Guide d'intégration HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

Guide de l'administrateur HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul

Ce manuel décrit la configuration et l'utilisation de l'intégration de Data Protector à HP StorageWorks Virtual Array, HP StorageWorks Enterprise Virtual Array, EMC Symmetrix Remote Data Facility et TimeFinder, ainsi que HP StorageWorks Disk Array XP. 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 HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul

Ce manuel décrit la configuration et l'utilisation de Data Protector en vue de réaliser une sauvegarde avec temps d'indisponibilité nul, une restauration instantanée et une restauration standard de bases de données Oracle, SAP R/3, Microsoft Exchange Server 2000/2003 et Microsoft SQL Server 2000. Ce manuel indique également comment configurer et utiliser Data Protector lors d'une sauvegarde ou d'une restauration à l'aide de Microsoft Volume Shadow Copy Service.

Guide de l'utilisateur HP OpenView Storage Data Protector MPE/iX System

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

Guide de l'utilisateur HP OpenView Storage Data Protector Media Operations

Ce manuel vous indique comment procéder au suivi et à la gestion des supports de stockage hors ligne. Il s'adresse aux administrateurs réseau responsables de la maintenance et de la sauvegarde de 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 OpenView Storage Data Protector

Ce manuel fournit une description des nouveautés de HP OpenView Storage Data Protector A.06.00. Il comporte également des informations sur les configurations prises en charges (périphériques, plates-formes et intégrations de bases de données en ligne, SAN et ZDB), des correctifs requis et des limitations, ainsi que des problèmes connus et de leurs solutions. Une version mise à jour des configurations prises en charge est disponible à l'adresse http://www.hp.com/support/manuals.

Il existe également quatre autres documents *Références, notes de publication et annonces produits* qui ont la même utilité pour les éléments suivants :

- Intégration OVO UNIX
- Intégration OVO 7.1x/7.2x Windows
- Intégration OVO 7.5 Windows
- Media Operations

Aide en ligne

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

Organisation de la documentation

Abréviations

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

Abréviation	**Manuel**
CLI	Guide de référence à l'interface de ligne de commande
Concepts	Guide conceptuel
DR	Guide de récupération après sinistre
GS	Guide de démarrage rapide
Aide	Aide en ligne
IG-IBM	Guide d'intégration—Applications IBM
IG-MS	Guide d'intégration—Applications Microsoft
IG-O/S	Guide d'intégration—Oracle, SAP R/3 et SAP DB/MaxDB
IG-OV	Guide d'intégration—HP OpenView Service Information Portal/OpenView Reporter
IG-OVOU	Guide d'intégration—HP OpenView Operations, UNIX
IG-OVOW	Guide d'intégration—HP OpenView Operations 7.1x, 7.2x, Windows
IG-OVOW	Guide d'intégration—HP OpenView Operations 7.5, Windows
IG-Var	Guide d'intégration—Sybase, Network Node Manager, NDMP et VMware
Install.	Guide d'installation et de choix des licences
MO GS	Guide de démarrage Media Operations
MO RN	Références, notes de publication et annonces produits Media Operations
MO UG	Guide de l'utilisateur Media Operations
MPE/iX	Guide de l'utilisateur MPE/iX System
PA	Références, notes de publication et annonces produits

Abréviation	Manuel
Dépan.	Guide de dépannage
ZDB Admin	Guide de l'administrateur ZDB
ZDB Concpt	Guide conceptuel ZDB
ZDB IG	Guide d'intégration ZDB

Tableau de documentation

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

								Guides d'intégration							ZDB			MO				
	Aide	**GS**	**Concepts**	**Install.**	**Dépan.**	**DR**	**PA**	**MS**	**O/S**	**IBM**	**Var**	**OV**	**OVOU**	**OVOW**	**Concpt**	**Admin**	**IG**	**GS**	**Utilisateur**	**PA**	**MPE/iX**	**CLI**
Sauvegarde	X	X	X					X	X	X	X				X	X	X				X	
CLI																						
Concepts/techniques	X							X	X	X	X	X	X	X		X	X				X	
Récupération après sinistre	X		X																			
Installation/mise à niveau	X	X					X					X	X	X				X	X		X	
Restauration instantanée	X		X												X		X					
Attribution de licences	X						X															
Limites	X				X		X	X	X	X	X			X			X			X		
Nouvelles fonctions	X																			X		
Stratégie de planification	X											X			X							
Procédures/tâches				X	X	X		X	X	X	X	X	X	X		X	X		X			
Recommandations			X				X								X					X		
Besoins				X			X	X	X	X	X			X				X	X	X		
Restauration	X	X	X					X	X	X	X					X	X				X	
Matrices de support							X															
Configurations prises en charge															X							
Dépannage	X			X				X	X	X	X	X				X	X					

Intégrations

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

Intégration	**Guide**
HP OpenView Operations (OVO)	IG-OVOU, IG-OVOW
HP OpenView Reporter (OVR)	IG-OV
HP OpenView Reporter Light	IG-OVOW
HP OpenView Service Information Portal (OVSIP)	IG-OV
HP StorageWorks Disk Array XP	tous les ZDB
HP StorageWorks Enterprise Virtual Array (EVA)	tous les ZDB
HP StorageWorks Virtual Array (VA)	tous les ZDB
IBM DB2 UDB	IG-IBM
Informix	IG-IBM
Lotus Notes/Domino	IG-IBM
Media Operations	MO Utilisateur
MPE/iX System	MPE/iX
Microsoft Exchange Servers	IG-MS, ZDB IG
Microsoft Exchange Single Mailbox	IG-MS
Microsoft SQL Server	IG-MS, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-MS, ZDB IG
NDMP Server	IG-Var
Network Node Manager (NNM)	IG-Var
Oracle	IG-O/S
Oracle ZDB	ZDB IG
SAP DB	IG-O/S
SAP R/3	IG-O/S, ZDB IG
Sybase	IG-Var

Intégration	**Guide**
Symmetrix (EMC)	tous les ZDB
VMware	IG-Var

Contenu des manuels

Le *Guide d'installation et de choix des licences HP OpenView Storage Data Protector* décrit l'installation du logiciel de sauvegarde réseau Data Protector, la configuration requise pour l'installation ainsi que des informations sur les mises à niveau et les licences.

Public

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

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

Organisation

Le manuel est organisé de la façon suivante :

Chapitre 1 “Présentation de la procédure d'installation” à la page 1.

Chapitre 2 “Installation de Data Protector sur votre réseau” à la page 17.

Chapitre 3 “Gestion de l'installation” à la page 195.

Chapitre 4 “Mise à niveau vers Data Protector A.06.00” à la page 247.

Chapitre 5 “Attribution de licences Data Protector” à la page 315.

Chapitre 6 “Résolution des problèmes d'installation” à la page 345.

Annexe A “Annexe A” à la page A-1.

Annexe B “Annexe B” à la page B-1.

1 Présentation de la procédure d'installation

Description du chapitre

Ce chapitre offre un aperçu de la procédure d'installation de Data Protector et du concept de l'installation. Il présente Data Protector, le Gestionnaire de cellule et l'interface graphique utilisateur de Data Protector.

Présentation de la procédure d'installation

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

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

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

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

Une cellule comprend généralement un Gestionnaire de cellule et de nombreux clients. Un système informatique devient un **client** Data Protector dès que vous le dotez de l'un des composants logiciels de Data Protector. Les composants client installés sur un système dépendent du rôle que joue ce système dans votre environnement de sauvegarde. Les composants Data Protector peuvent être installés localement sur un système unique ou distribués sur de nombreux systèmes à partir des Serveurs d'installation.

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

Le composant **Agent de disque** Data Protector doit être installé sur les systèmes client dotés de disques devant être sauvegardés. L'Agent de disque vous permet en effet de sauvegarder des données à partir du disque client ou de les restaurer.

Présentation de la procédure d'installation

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

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

✓ Le système sur lequel le Gestionnaire de cellule sera installé. Pour connaître les systèmes d'exploitation et les différentes versions pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

Chaque cellule ne peut comporter qu'un Gestionnaire de cellule. Vous ne pouvez pas exécuter Data Protector si vous n'avez pas installé un Gestionnaire de cellule.

✓ Les systèmes qui seront utilisés pour accéder aux fonctions de Data Protector via l'interface utilisateur, et qui doivent être dotés du composant Interface utilisateur.

✓ Les systèmes qui seront sauvegardés et qui doivent être dotés du composant Agent de disque pour la sauvegarde des systèmes de fichiers et du composant Agent d'application approprié pour les intégrations de bases de données en ligne.

✓ Les systèmes auxquels seront connectés les périphériques de sauvegarde et qui requièrent un composant Agent de support.

✓ Le ou les systèmes sur lesquels le Serveur d’installation Data Protector sera installé. Deux types de Serveurs d'installation (IS) sont disponibles pour l'installation des logiciels distants : l'un pour les clients UNIX et l'autre pour les clients Windows. Chacun doit être installé sur la plate-forme à laquelle il correspond.

Le choix de l'ordinateur utilisé comme Serveur d’installation est indépendant du Gestionnaire de cellule et du ou des systèmes sur lesquels l'Interface utilisateur est installée. Le Gestionnaire de cellule et le Serveur d’installation peuvent se trouver sur le même système (s'ils sont tous deux destinés à la même plate-forme) ou sur des systèmes différents.

Un Serveur d'installation peut être partagé par plusieurs cellules Data Protector.

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

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

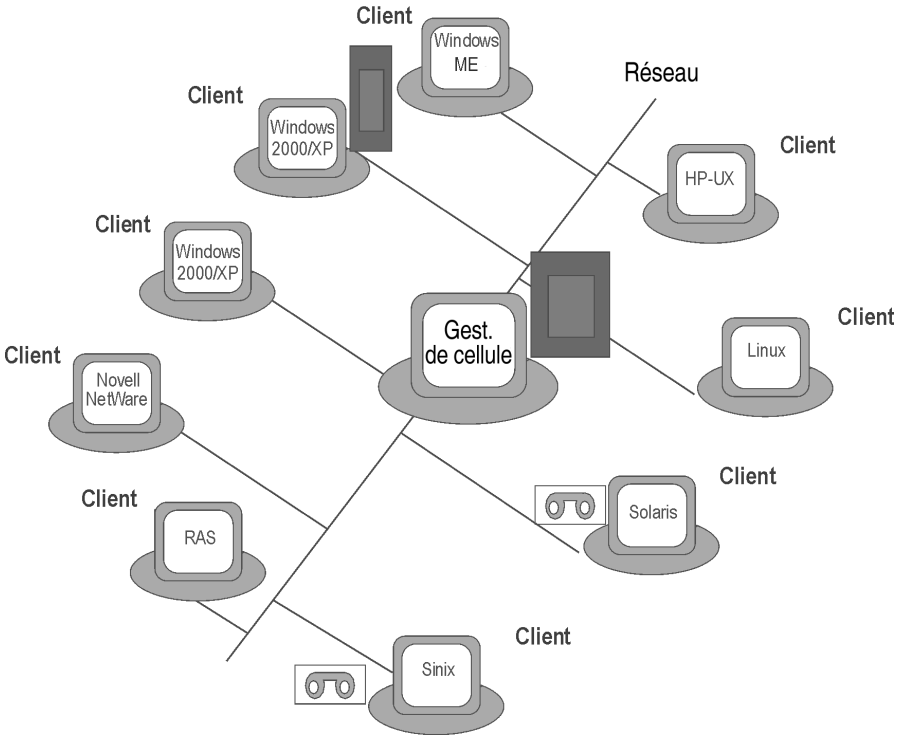
Une fois que vous avez déterminé les rôles des systèmes dans votre future cellule Data Protector, la procédure d'installation comprend les étapes générales suivantes :

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

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

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

Figure 1-1 Cellule Data Protector



Concept d'installation

Une fois que vous avez installé le Gestionnaire de cellule de Data Protector, l'Interface utilisateur et le Serveur d'installation (un de ces éléments au moins est nécessaire pour chaque plate-forme, UNIX et Windows), vous pouvez distribuer le logiciel Data Protector aux clients utilisant des systèmes d'exploitation pour lesquels l'installation à distance est prise en charge. Reportez-vous à la figure 1-2 à la page 8.

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

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

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

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

A partir d'un Serveur d'installation pour UNIX (pour obtenir une liste des plates-formes prises en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*), vous pouvez installer à distance un logiciel client sur HP-UX, Solaris, Sinix, Linux, AIX et tout autre système d'exploitation UNIX pris en charge.

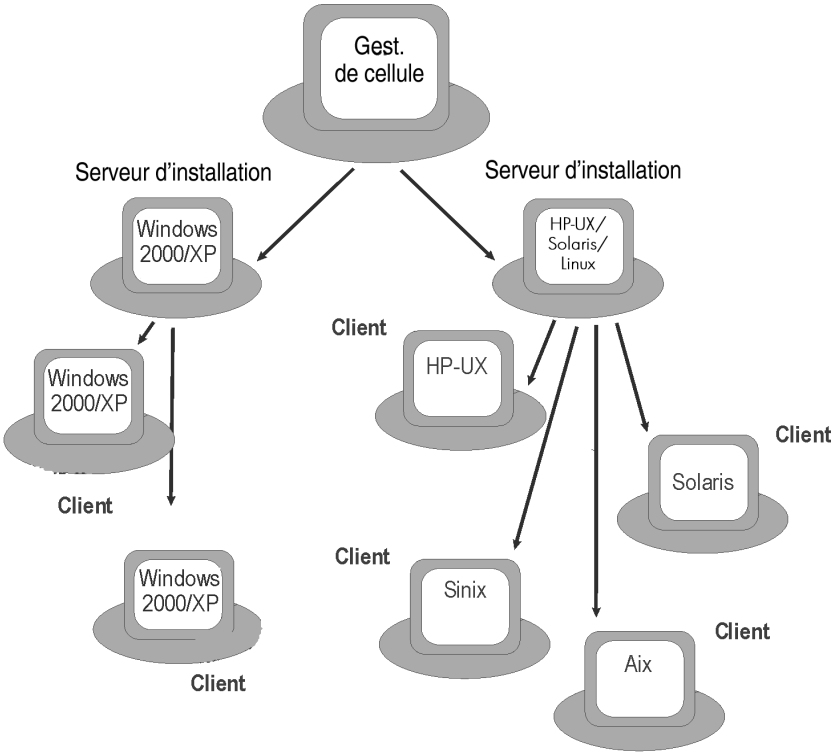
Pour les systèmes d'exploitation UNIX pour lesquels l'installation à distance n'est pas prise en charge, ou si vous n'installez pas un Serveur d'installation pour UNIX, vous pouvez installer les clients UNIX localement, à partir du DVD-ROM d'installation de Data Protector UNIX.

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

Pour plus d'informations sur les méthodes d'installation disponibles pour les différents clients Data Protector, reportez-vous à la section “Installation des clients Data Protector” à la page 50.

Pour connaître la procédure d'installation locale des clients UNIX, reportez-vous à la section “Installation locale de clients UNIX” à la page 130.

Figure 1-2 Concept d'installation de Data Protector



DVD-ROM d'installation de Data Protector

Data Protector prend en charge différents systèmes d'exploitation sur plusieurs architectures de processeur. Par conséquent, 2 DVD-ROM sont nécessaires pour couvrir toutes les plates-formes. Pour plus de détails sur le contenu des différents DVD-ROM, reportez-vous à la section “Liste des DVD-ROM Data Protector” à la page 9.

REMARQUE Le meilleur support d'installation pour Data Protector est le DVD-ROM. Si vous effectuez l'installation à partir de CD-ROM au lieu de DVD-ROM, reportez-vous également à l'"Annexe C," à la page C-1, dans laquelle vous trouverez une liste de CD-ROM et les différences dans la procédure d'installation.

Tableau 1-1 Liste des DVD-ROM Data Protector

N° de DVD	Titre du DVD-ROM	Sommaire
1	Pack Starter Data Protector pour Windows Comprend Open File Backup (sauvegarde des fichiers ouverts), Media Operations, et les agents pour les clients NetWare, MPE et OpenVMS	• Gestionnaire de cellule et Serveur d'installation pour Windows sur les systèmes 32 bits et 64 bits (AMD64/Intel EM64T) • AutoPass[a] • Tous les manuels en anglais au format PDF (dans le répertoire DOCS) • Clients Windows IA64 • Clients Novell NetWare • Clients OpenVMS (systèmes Alpha et IA64) • Clients MPE • Package d'installation Open File Manager • Produit de démonstration pour plates-formes Windows • Informations sur le produit • Package d'installation pour Media Operations

Tableau 1-1 Liste des DVD-ROM Data Protector

N° de DVD	Titre du DVD-ROM	Sommaire
2	Pack Starter Data Protector pour HP-UX, Solaris et Linux Comprend des agents pour les clients HP-UX, Solaris et Linux	• Gestionnaire de cellule et Serveur d'installation pour HP-UX (PA-RISC, IA64), Solaris et Linux • Clients pour d'autres systèmes UNIX • AutoPass[b] • Tous les manuels en anglais au format PDF (dans le répertoire DOCS) • Packages d'intégration OpenView

a. AutoPass n'est pas disponible sur les systèmes d'exploitation Windows x64.
b. AutoPass n'est pas disponible sous Linux.

Choix du système Gestionnaire de cellule

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

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

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

✓ Plates-formes prises en charge

Vous pouvez installer le Gestionnaire de cellule sur la plate-forme Windows, HP-UX ou Solaris. Pour obtenir plus d'informations sur les versions/éditions de ces plates-formes qui sont prises en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

✓ Fiabilité du système Gestionnaire de cellule

Dans la mesure où le Gestionnaire de cellule contient la base de données IDB et où la sauvegarde et la restauration sont impossibles en cas de panne du Gestionnaire de cellule, il est important de choisir un système très fiable pour cette installation.

✓ Croissance de la base de données et espace disque nécessaire

Le Gestionnaire de cellule contient la base de données interne (IDB) de Data Protector. Celle-ci comprend des informations sur les données sauvegardées et les supports correspondants, sur les messages de session et sur les périphériques. En fonction de votre environnement, la base peut atteindre une taille significative. Par exemple, si la majorité des sauvegardes concerne des systèmes de fichiers, la taille habituelle de la base IDB *estimée* représente 2 % de

l'espace disque occupé par les données sauvegardées. Vous pouvez utiliser le tableau `IDB_capacity_planning.xls` (présent sur le support d'installation de Data Protector) afin d'estimer la taille de la base de données IDB.

Reportez-vous à l'index de l'aide en ligne (rubrique “croissance et performances de l'IDB“) pour plus d'informations sur la planification et la gestion de la taille et de la croissance de la base de données.

Pour plus d'informations sur l'espace disque requis pour la base de données IDB, reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

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

Etape suivante Pour connaître la configuration requise de votre futur système Gestionnaire de cellule, reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d’installation (IS) de Data Protector” à la page 19.

Choix du système de l'interface utilisateur de Data Protector

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

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

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

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

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

Pour utiliser la fonctionnalité d'interface graphique utilisateur de Data Protector sur les plates-formes Gestionnaire de cellule UNIX pour lesquelles l'interface graphique utilisateur de Data Protector n'est pas prise en charge, utilisez la commande `omniusers` pour créer un compte utilisateur distant sur le Gestionnaire de cellule. Vous pouvez alors utiliser le compte utilisateur créé avec l'interface graphique utilisateur de Data Protector installée pour lancer l'interface et se connecter au Gestionnaire de cellule. Pour plus de détails, reportez-vous à la page de manuel `omniusers`.

Pour plus d'informations sur les versions/éditions des systèmes d'exploitation pris en charge pour l'interface utilisateur, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*. Pour plus d'informations sur la prise en charge des différentes langues et l'utilisation de caractères non-ASCII dans les noms de fichier, recherchez dans l'index de l'aide en ligne : “paramètres de langue, personnalisation”.

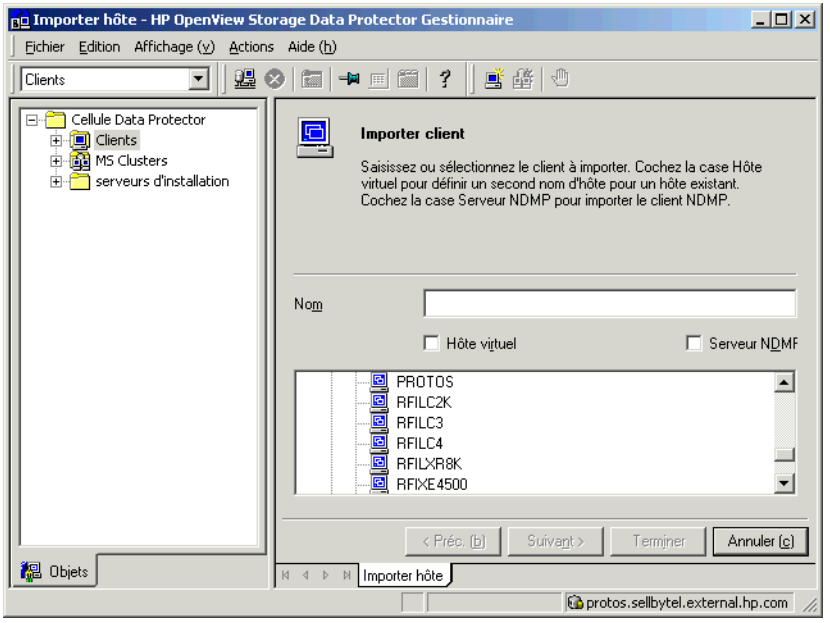
Une fois l'interface utilisateur installée sur un système de la cellule, vous pouvez accéder à distance au Gestionnaire de cellule à partir de ce système. Vous n'êtes pas obligé d'utiliser l'interface graphique utilisateur sur le Gestionnaire de cellule.

Interface graphique utilisateur de Data Protector

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

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

Figure 1-3 Interface graphique utilisateur de Data Protector



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

REMARQUE

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

2 Installation de Data Protector sur votre réseau

Description du chapitre

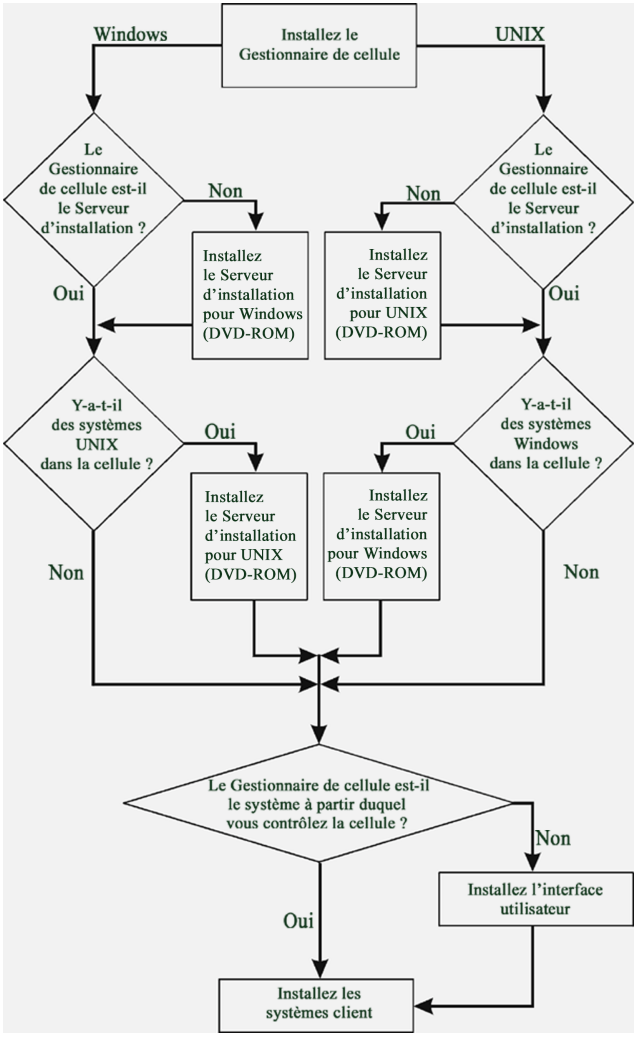
Ce chapitre contient des instructions détaillées sur les opérations suivantes :

- Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector. Reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector” à la page 19.
- Installation des clients Data Protector. Reportez-vous à la section “Installation des clients Data Protector” à la page 50.
- Installation de l'interface utilisateur localisée de Data Protector. Reportez-vous à la section “Installation de l'interface utilisateur localisée de Data Protector” à la page 168.
- Installation de l'Edition serveur unique Data Protector. Reportez-vous à la section “Installation de l'Edition serveur unique de Data Protector” à la page 173.
- Installation des Rapports Web Data Protector. Reportez-vous à la section “Installation du composant Rapports Web de Data Protector” à la page 175.
- Installation de Data Protector sur MC/ServiceGuard. Reportez-vous à la section “Installation de Data Protector sur MC/ServiceGuard” à la page 177.
- Installation de Data Protector sur Microsoft Cluster Server. Reportez-vous à la section “Installation de Data Protector sur Microsoft Cluster Server” à la page 179.
- Installation de clients Data Protector sur un cluster Veritas. Reportez-vous à la section “Installation de clients Data Protector sur un cluster Veritas” à la page 190.
- Installation de clients Data Protector sur un cluster Novell NetWare. Reportez-vous à la section “Installation de clients Data Protector sur un cluster Novell NetWare” à la page 191.

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

Pour connaître le déroulement de la procédure d'installation, reportez-vous à la figure 2-1 :

Figure 2-1 Procédure d'installation



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

IMPORTANT

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

REMARQUE

Les procédures de ce chapitre pour l'installation du Gestionnaire de cellule et du Serveur d'installation et pour l'installation locale des clients supposent l'utilisation d'un DVD-ROM comme support d'installation. Si vous utilisez un CD-ROM comme support, consultez également l'"Annexe C," à la page C-1, qui fournit une liste des CD-ROM et indique les différences dans la procédure d'installation.

Installation d'un Gestionnaire de cellule UNIX

Cette section fournit des instructions détaillées sur la procédure d'installation d'un Gestionnaire de cellule UNIX. Si vous souhaitez n'installer que le Gestionnaire de cellule Windows, reportez-vous à la section "Installation d'un Gestionnaire de cellule Windows" à la page 31.

Configuration système requise

- Le système HP-UX, Solaris ou Linux qui deviendra le Gestionnaire de cellule doit :

  ✓ Disposer d'un espace disque suffisant pour le logiciel Data Protector. Pour plus de détails à ce sujet, reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*. Pour surmonter les problèmes de manque d'espace, vous pouvez effectuer l'installation sur des répertoires liés ; reportez-vous au préalable aux sections "Structure des répertoires installés sous HP-UX, Solaris et Linux" à la page 26 et "Allocation d'espace disque supplémentaire pour l'installation du Gestionnaire de cellule" à la page 30.

  ✓ Disposer d'un espace disque suffisant (équivalent à environ 2 % des données à sauvegarder) pour la base de données IDB. Pour plus de détails à ce sujet, reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage*

Data Protector. Notez que la conception actuelle de la base de données IDB permet de déplacer les fichiers binaires si la croissance de la base de données rend cette opération nécessaire. Dans l'index de l'aide en ligne, recherchez : "base de données interne (IDB), calcul de la taille".

- ✓ Prendre en charge les noms de fichiers longs. Pour vérifier si votre système de fichiers prend en charge les noms de fichiers longs, utilisez la commande `getconf NAME_MAX <répertoire>`.
- ✓ Disposer du démon `inetd`, lequel doit être opérationnel.
- ✓ Disposer du port numéro 5555 (par défaut). Si ce n'est pas le cas, reportez-vous à la section “Modification du numéro de port par défaut” à la page B-30.
- ✓ Disposer du protocole TCP/IP, lequel doit être en cours d'exécution. Ce protocole doit pouvoir résoudre les noms d'hôte.
- ✓ Avoir accès à un lecteur de DVD-ROM.
- ✓ Reconnaître le Gestionnaire de cellule, en cas d'utilisation d'un serveur NIS. Reportez-vous à la section “Préparation d'un serveur NIS” à la page B-32.
- ✓ Disposer du shell `ksh`.

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

REMARQUE

L'interface graphique n'est pas prise en charge sous Linux. Toutefois, vous pouvez utiliser la commande `omniusers` pour créer un compte utilisateur distant sur le nouveau Gestionnaire de cellule. Vous pouvez alors utiliser ce compte utilisateur avec l'interface graphique utilisateur de Data Protector installée pour lancer l'interface et vous connecter au nouveau Gestionnaire de cellule. Reportez-vous à la page `omniusers` du manuel.

Gestionnaire de cellule compatible cluster

D'autres conditions et étapes sont requises pour l'installation d'un Gestionnaire de cellule compatible cluster. Reportez-vous à la section “Installation d'un Gestionnaire de cellule compatible cluster” à la page 177.

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

Définition des paramètres de noyau

Sous HP-UX, il est recommandé de régler le paramètre de noyau `maxdsiz` (taille maximale des segments de données) sur au moins 134 217 728 octets (128 Mo), et le paramètre de noyau `semmnu` (nombre de structures Undo de sémaphore) sur au moins 256 Mo. Une fois ces modifications effectuées, recompilez le noyau et redémarrez la machine.

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

Procédure d'installation

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

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

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

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

   Par exemple :

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

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

- Pour copier sur votre disque local les répertoires DP_DEPOT, AUTOPASS et LOCAL_INSTALL, à l'emplacement où sont stockés les fichiers d'installation, exécutez les commandes suivantes :

  ```
  mkdir <répertoire>
  cp -r /dvdrom/<rép_plateforme>/DP_DEPOT <répertoire>
  cp -r /dvdrom/<rép_plateforme>/AUTOPASS <répertoire>
  cp -r /dvdrom/<rép_plateforme>/LOCAL_INSTALL
  <répertoire>
  ```

  Où *<rép_plateforme>* est :

hpux_ia	HP-UX 11.23 sur les systèmes IA-64
hpux_pa	HP-UX sur les systèmes PA-RISC
linux_x86_64	Systèmes Linux avec AMD64/Intel EM64T
solaris	Systèmes Solaris

- Pour copier l'ensemble du DVD-ROM sur votre disque local, exécutez la commande :

  ```
  cp -r /dvdrom <rép_image_dvd>
  ```

2. Exécutez la commande omnisetup.sh.

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

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

   Pour lancer l'installation à partir du disque :

   - Si vous avez copié les répertoires DP_DEPOT, AUTOPASS et LOCAL_INSTALL sur votre disque local dans le répertoire *<répertoire>*, exécutez les commandes :

     ```
     cd <répertoire>/LOCAL_INSTALL
     ./omnisetup.sh -source <répertoire> -CM
     ```

   - Si vous avez copié l'ensemble du DVD-ROM dans *<rép_image_dvd>*, exécutez la commande omnisetup.sh avec le paramètre -CM :

     ```
     cd <rép_image_dvd>/LOCAL_INSTALL
     ./omnisetup.sh -CM
     ```

3. ***Sous HP-UX et Solaris,*** `omnisetup.sh` vous invite à installer ou à mettre à niveau l'utilitaire HP OpenView AutoPass, si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à la section “Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP OpenView AutoPass” à la page 334. L'installation d'AutoPass est recommandée.

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

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

   Sous Linux, HP OpenView AutoPass n'est pas installé.

REMARQUE

Si vous avez installé/mis à niveau le Gestionnaire de cellule sous Solaris 9 ou 10, installez l'Agent de disque à distance sur le Gestionnaire de cellule après l'installation/la mise à niveau à l'aide d'un Serveur d'installation. L'Agent de disque générique Solaris sera ainsi remplacé par l'Agent de disque Solaris 9 ou Solaris 10. Reportez-vous à la section “Installation distante de clients Data Protector” à la page 54 ou à la page de manuel `ob2install`.

Si vous souhaitez installer un Serveur d'installation pour UNIX sur votre Gestionnaire de cellule, vous pouvez le faire à ce stade. Pour plus de détails sur les étapes requises, reportez-vous à la section “Installation des Serveurs d'installation pour UNIX” à la page 40.

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

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

IMPORTANT

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

`/opt/omni/ -> /<préfixe>/opt/omni/`

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

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

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

Pour plus d'informations, reportez-vous à la section “Allocation d'espace disque supplémentaire pour l'installation du Gestionnaire de cellule” à la page 30.

`/opt/omni/bin`	Toutes les commandes
`/opt/omni/gui`	Eléments de l'interface graphique utilisateur
`/opt/omni/gui/help`	Fichiers d'aide en ligne
`/opt/omni/lbin`	Commandes internes de Data Protector
`/opt/omni/sbin`	Commandes super-utilisateur
`/opt/omni/sbin/install`	Scripts d'installation
`/etc/opt/omni`	Informations de configuration
`/opt/omni/lib`	Bibliothèques partagées pour la compression, le codage de données et la gestion de périphériques
`/opt/omni/doc/C`	Documentation en ligne (facultatif)
`/var/opt/omni/log` et `/var/opt/omni/server/log`	Fichiers journaux

`/opt/omni/lib/nls/C`	Fichiers catalogue de messages
`/opt/omni/lib/man`	Pages de manuel
`/var/opt/omni/tmp`	Fichiers temporaires
`/var/opt/omni/server/db40`	Fichiers IDB. Pour plus de détails, recherchez dans l'index de l'aide en ligne : "IDB, emplacement des répertoires".

Configuration du démarrage et de l'arrêt automatiques

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

Les fichiers suivants sont configurés automatiquement :

HP-UX :

`/sbin/init.d/omni`	Script contenant les procédures de démarrage et d'arrêt.
`/sbin/rc1.d/K162omni`	Lien vers le script `/sbin/init.d/omni` qui permet d'arrêter Data Protector.
`/sbin/rc2.d/S838omni`	Lien vers le script `/sbin/init.d/omni` qui permet de démarrer Data Protector.
`/etc/rc.config.d/omni`	Contient une variable `omni` définissant : `omni=1` Data Protector est arrêté et démarré automatiquement au réamorçage du système. C'est l'option par défaut. `omni=0` Data Protector n'est pas arrêté et démarré automatiquement au réamorçage du système.

Solaris :

`/etc/init.d/omni`	Script contenant les procédures de démarrage et d'arrêt.

`/etc/rc1.d/K09omni`	Lien vers le script `/etc/init.d/omni` qui permet d'arrêter Data Protector.
`/etc/rc2.d/S97omni`	Lien vers le script `/etc/init.d/omni` qui permet de démarrer Data Protector.

Linux :

`/etc/init.d/omni`	Script contenant les procédures de démarrage et d'arrêt.
`/etc/rc`*`<niveau_init>`*`.d/K10omni`	Lien vers le script `/etc/init.d/omni` qui permet d'arrêter Data Protector. Où *`<niveau_init>`* est égal à 1 ou 6.
`/etc/rc`*`<niveau_init>`*`.d/S90omni`	Lien vers le script `/etc/init.d/omni` qui permet de démarrer Data Protector. Où *`<niveau_init>`* est égal à 2, 3, 4 ou 5.

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

HP-UX :

`/etc/services`	Le numéro de port Data Protector du service est ajouté au fichier.
`/opt/omni/lbin/crs`	Le service CRS de Data Protector est ajouté.

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

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

`/opt/omni/lbin/rds`	Le service Data Protector `Raima Database Server (RDS)` s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Le RDS gère la base de données IDB.
`/opt/omni/lbin/mmd`	Le service `Media Management Daemon (MMD)` de Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Il gère les opérations de gestion des périphériques et des supports.

Configuration des variables d'environnement

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

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

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

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

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

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

REMARQUE

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

"personnalisation des paramètres de langue") pour plus d'informations sur la personnalisation des paramètres de langue dans l'interface graphique de Data Protector.

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

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

- Si vous disposez d'un disque contenant suffisamment d'espace et monté en tant que `/data_protector`, créez le lien suivant vers `opt/omni` :

  ```
  mkdir /data_protector/opt_omni
  ```

  ```
  ln -s /data_protector/opt_omni /opt/omni
  ```

  Répétez cette opération pour tout autre répertoire que vous souhaitez lier, par exemple `/var/opt/omni` et `/etc/opt/omni`.

- ***Sous HP-UX***, si vous disposez d'un système de fichiers non monté `/dev/vgspare/lvol2`, procédez comme suit :

  ```
  mkdir /opt/omni
  ```

  ```
  mount /dev/vgspare/lvol2 /opt/omni
  ```

- ***Sous Solaris***, si vous disposez d'un système de fichiers non monté `/dev/dsk/c0t0d0s0`, procédez comme suit :

  ```
  mkdir /opt/omni
  ```

  ```
  montez /dev/dsk/c0t0d0s0 /opt/omni
  ```

Etape suivante

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

1. Si vous n'avez pas installé un Serveur d'installation pour UNIX sur le même système, reportez-vous à la section "Installation des Serveurs d'installation pour UNIX" à la page 40.
2. Installez un Serveur d'installation pour Windows, si vous souhaitez effectuer une installation à distance sur des clients Windows. Reportez-vous à la section "Installation d'un Serveur d'installation pour Windows" à la page 44.
3. Distribuez le logiciel aux clients. Reportez-vous à la section "Installation des clients Data Protector" à la page 50.

Installation d'un Gestionnaire de cellule Windows

Configuration requise

Le système Windows qui deviendra votre Gestionnaire de cellule doit répondre aux critères suivants :

- ✓ Etre doté d'une version du système d'exploitation Windows prise en charge. Reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector* pour connaître les versions de système d'exploitation prises en charge pour le Gestionnaire de cellule.
- ✓ Disposer de Microsoft Internet Explorer 5.0 ou supérieur.
- ✓ Disposer d'un espace disque suffisant pour le logiciel Gestionnaire de cellule de Data Protector. Pour plus de détails à ce sujet, reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage Data Protector* .
- ✓ Disposer d'un espace disque suffisant (équivalent à environ 2 % des données sauvegardées) pour la base de données IDB. Pour plus de détails à ce sujet, reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage Data Protector* .
- ✓ Disposer du port numéro 5555 (par défaut). Si ce n'est pas le cas, reportez-vous à la section "Modification du numéro de port par défaut" à la page B-30.

- ✓ Disposer d'une adresse IP fixe pour le système sur lequel le Gestionnaire de cellule doit être installé. Si le système est configuré en tant que client DHCP, son adresse IP change ; il est donc nécessaire soit d'attribuer une entrée DNS permanente au système (et de le reconfigurer), soit de configurer un serveur DHCP afin de réserver une adresse IP fixe pour le système (l'adresse IP est liée à l'adresse MAC du système).
- ✓ Disposer de l'implémentation Microsoft du protocole TCP/IP, lequel doit être installé et en cours d'exécution. Ce protocole doit pouvoir résoudre les noms d'hôte. Les noms de l'ordinateur et de l'hôte doivent être identiques. Reportez-vous à la section “Paramétrage du protocole TCP/IP sur les systèmes Windows” à la page B-21 pour obtenir des informations sur l'installation et la configuration du protocole TCP/IP.
- ✓ Avoir accès à un lecteur de DVD-ROM.

Client Microsoft Terminal Services

- ✓ Si vous souhaitez installer Data Protector sous Windows via Microsoft Terminal Services Client, le `Mode Terminal Server` du système où vous installez Data Protector doit être défini sur `Administration distante` :

  1. Dans le Panneau de configuration de Windows, cliquez sur `Outils d'administration`, puis sur `Configuration des services Terminal Server`.
  2. Dans la boîte de dialogue `Configuration Terminal Server`, cliquez sur `Paramètres du serveur`. Vérifiez que le serveur Terminal Services s'exécute dans le mode administration distante.

Recommandation

Avant de procéder à l'installation de Data Protector A.06.00, assurez-vous que vous disposez de Microsoft Installer (MSI) 2.0. Si vous possédez une version plus ancienne de MSI, le programme d'installation de Data Protector va automatiquement le mettre à niveau avec la version 2.0. Dans ce cas, Data Protector affichera une remarque à la fin de l'installation, indiquant que MSI a été mis à niveau. Si MSI a été mis à niveau, il est vivement recommandé de redémarrer le système.

Il est recommandé de mettre MSI à niveau vers la version 2.0 avant d'installer Data Protector A.06.00.

Gestionnaire de cellule compatible cluster

D'autres conditions et étapes sont requises pour l'installation d'un Gestionnaire de cellule compatible cluster. Reportez-vous à la section “Installation d'un Gestionnaire de cellule compatible cluster” à la page 179.

Procédure d'installation

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

1. Insérez le DVD-ROM d'installation Windows et exécutez :

   Systèmes 32 bits : `\Windows_other\i386\setup.exe`

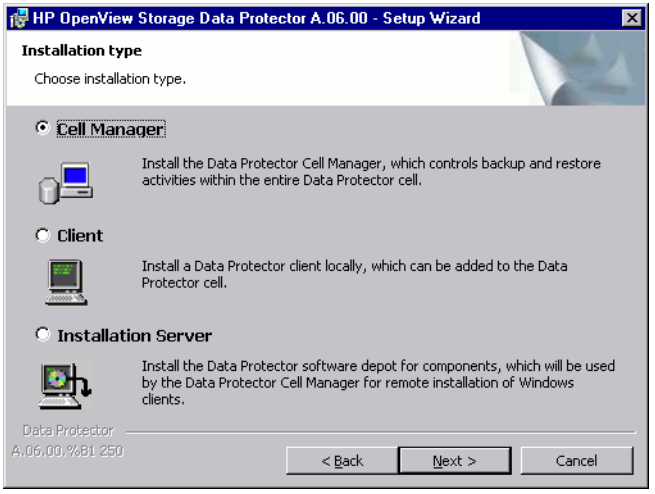
   Systèmes 64 bits : `\Windows_other\x8664\setup.exe`

   L'assistant d'installation de Data Protector s'affiche.

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

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

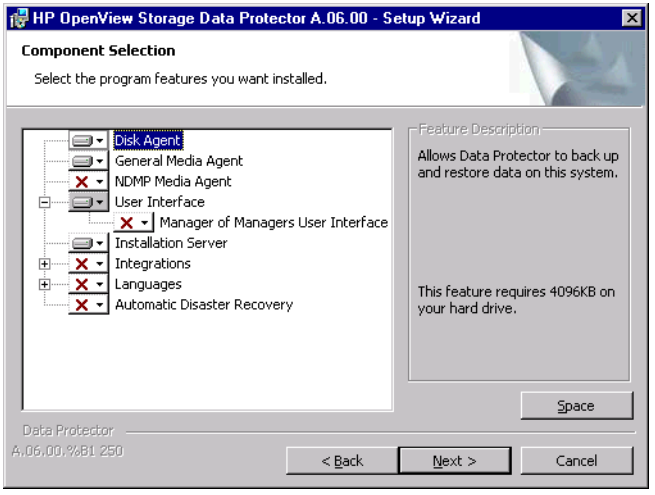
Figure 2-2 **Sélection du type d'installation**



4. Indiquez le nom de l'utilisateur et le mot de passe du compte sur lequel les services Data Protector s'exécuteront. Cliquez sur `Suivant` pour continuer.
5. Cliquez sur `Suivant` pour installer Data Protector dans le répertoire par défaut.

   Sinon, cliquez sur `Modifier` pour ouvrir la fenêtre `Modifier le dossier de destination actuel` et entrez un autre chemin.
6. Dans la page `Sélection des composants`, sélectionnez les composants à installer. Pour obtenir la liste et les descriptions des composants Data Protector, reportez-vous à la section "Composants Data Protector" à la page 63.

Figure 2-3 **Sélection des composants logiciels**



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

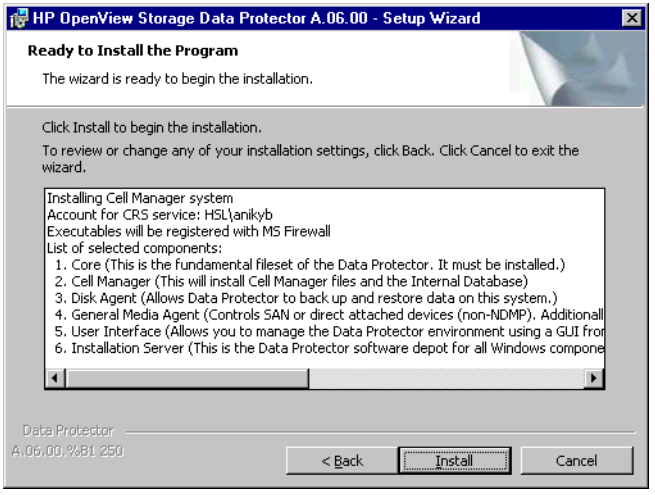
7. ***Windows XP SP2, Windows 2003 SP1 :*** si Data Protector détecte le pare-feu Windows sur votre système, la page Configuration du pare-feu Windows est affichée. Data Protector enregistrera tous les exécutables Data Protector nécessaires. Par défaut, l'option `Permettre initialement aux nouveaux fichiers binaires Data Protector enregistrés d'ouvrir des ports le cas`

échéant est sélectionnée. Si vous ne souhaitez pas activer Data Protector pour les ports ouverts, désélectionnez l'option. Toutefois, notez que les exécutables doivent être activés pour que Data Protector fonctionne correctement.

Cliquez sur Suivant.

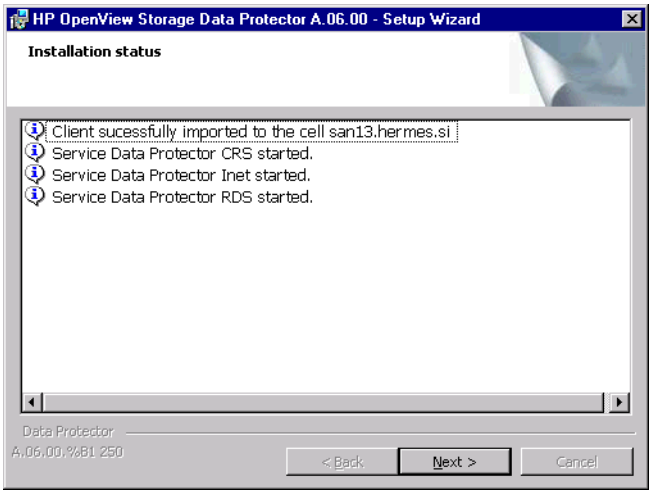
8. La liste des composants sélectionnés s'affiche. Cliquez sur Installer pour démarrer l'installation des composants sélectionnés. L'installation peut durer plusieurs minutes.

Figure 2-4 Liste des composants sélectionnés



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

Figure 2-5 Page d'état de l'installation



10. ***Sur les systèmes d'exploitation autres que Windows x64***, l'assistant d'installation vous permet d'installer ou de mettre à niveau l'utilitaire HP OpenView Auto Pass, si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à la section "Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP OpenView AutoPass" à la page 334.

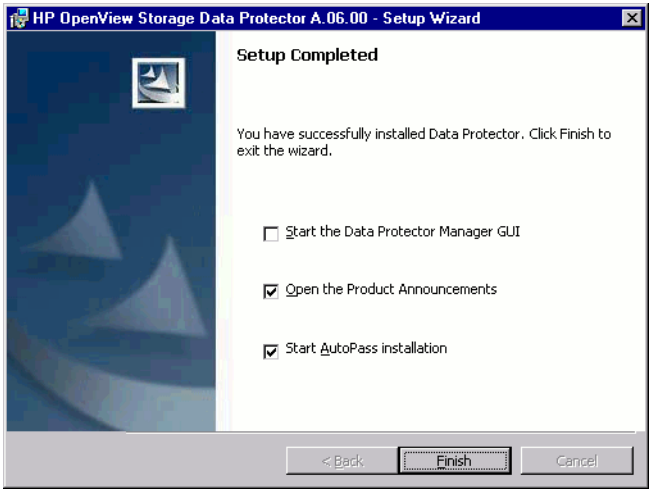
    Par défaut, l'option `Start AutoPass installation (Démarrer l'installation d'AutoPass)` ou `Upgrade AutoPass installation (Mettre à niveau l'installation d'AutoPass)` est sélectionnée. L'installation de l'utilitaire HP OpenView AutoPass est recommandée. Si vous ne souhaitez pas installer ou mettre à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

    Sur les systèmes d'exploitation Windows x64, AutoPass n'est pas installé.

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

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

Figure 2-6 Sélection de l'installation d'AutoPass



Cliquez sur `Terminer`.

Après l'installation

Dès la fin de l'installation, les fichiers du Gestionnaire de cellule se trouvent dans le répertoire *<répertoire_Data_Protector>*`\bin` et le dépôt de logiciel pour Windows se trouve dans le répertoire *<répertoire_Data_Protector>*`\Depot`.

A la fin de l'installation, les processus suivants s'exécutent sur le Gestionnaire de cellule dans le répertoire *<répertoire_Data_Protector>*`\bin` :

`crs.exe`	Le service Cell Request Server (CRS) de Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé

	sur le système. Il lance et contrôle les sessions de sauvegarde et de restauration dans la cellule.
`rds.exe`	Le service Raima Database Server (RDS) de Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Le RDS gère la base de données IDB.
`omniinet.exe`	Le service résident de Data Protector qui permet la communication avec les services Data Protector installés sur les autres systèmes du réseau. Le service `Inet de Data Protector` doit s'exécuter sur tous les systèmes de la cellule Data Protector.

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

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

Résolution des problèmes

Si l'installation a échoué, contrôlez la configuration vérifiée par le `processus d'installation` lui-même, et essayez de déterminer les causes de l'échec si la configuration n'a pas été respectée. Reportez-vous à la section “Configuration requise” à la page 31.

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

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

Etape suivante

A ce stade, le Gestionnaire de cellule est installé et, si vous l'avez sélectionné, le Serveur d'installation pour Windows l'est également. Tâches suivantes :

1. Installez le Serveur d'installation pour UNIX, si votre environnement de sauvegarde est mixte. Reportez-vous à la section “Installation des Serveurs d'installation” à la page 39. Ne tenez pas compte de cette étape si vous n'avez pas besoin du Serveur d'installation pour UNIX.
2. Distribuez le logiciel aux clients. Reportez-vous à la section “Installation des clients Data Protector” à la page 50.

Installation des Serveurs d'installation

Les Serveurs d'installation peuvent être installés sur le système du Gestionnaire de cellule ou sur tout système pris en charge et connecté au Gestionnaire de cellule par un réseau local. Reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector* pour connaître les versions de système d'exploitation prises en charge pour le Serveur d'installation.

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

Installation des Serveurs d'installation pour UNIX

Configuration requise sous UNIX

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

- ✓ Disposer du système d'exploitation HP-UX, Solaris ou Linux. Pour obtenir des informations sur les systèmes d'exploitation pris en charge pour le Serveur d'installation, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.
- ✓ Disposer du démon `inetd`, lequel doit être opérationnel.
- ✓ Disposer du port numéro 5555 (par défaut). Si ce n'est pas le cas, reportez-vous à la section "Modification du numéro de port par défaut" à la page B-30.
- ✓ Disposer du protocole TCP/IP, lequel doit être en cours d'exécution. Ce protocole doit pouvoir résoudre les noms d'hôte.
- ✓ Disposer d'un espace disque suffisant pour l'intégralité du dépôt de logiciel de Data Protector. Pour plus de détails à ce sujet, reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage Data Protector* .
- ✓ Disposer d'un lecteur de DVD-ROM.
- ✓ Le Gestionnaire de cellule de la cellule Data Protector doit être mis à niveau vers la version A.06.00.

IMPORTANT

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

`/opt/omni/ -> /<préfixe>/opt/omni/`

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

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

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

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

Procédure d'installation

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

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

   Par exemple :

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

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

   - Pour copier sur votre disque local les répertoires `DP_DEPOT`, `AUTOPASS` et `LOCAL_INSTALL`, à l'emplacement où sont stockés les fichiers d'installation, exécutez les commandes suivantes :

     ```
     mkdir <répertoire>
     cp -r /dvdrom/<rép_plateforme>/DP_DEPOT <répertoire>
     cp -r /dvdrom/<rép_plateforme>/AUTOPASS <répertoire>
     cp -r /dvdrom/LOCAL_INSTALL <répertoire>
     ```

     Où *<rép_plateforme>* est :

`hpux_ia`	HP-UX 11.23 sur les systèmes IA-64
`hpux_pa`	HP-UX sur les systèmes PA-RISC
`linux_x86_64`	Systèmes Linux avec AMD64/Intel EM64T
`solaris`	Systèmes Solaris

   - Pour copier l'ensemble du DVD-ROM sur votre disque local, exécutez la commande :

     ```
     cp -r /dvdrom <rép_image_dvd>
     ```

2. Exécutez la commande `omnisetup.sh`.

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

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

Pour lancer l'installation à partir du disque :

- Si vous avez copié les répertoires `DP_DEPOT`, `AUTOPASS` et `LOCAL_INSTALL` sur votre disque local dans le répertoire *<répertoire>*, exécutez les commandes :

  ```
  cd <répertoire>/LOCAL_INSTALL
  ./omnisetup.sh -source <répertoire> -IS
  ```

- Si vous avez copié l'ensemble du DVD-ROM dans *<rép_image_dvd>*, exécutez la commande `omnisetup.sh` avec le paramètre `-IS` :

  ```
  cd <rép_image_dvd>/LOCAL_INSTALL
  ./omnisetup.sh -IS
  ```

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

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

La commande `omnisetup.sh` installe le Serveur d'installation avec tous les packages. Pour installer certains packages uniquement, utilisez la commande `swinstall` (HP-UX), `pkgadd` (Solaris) ou `rpm` (Linux). Reportez-vous à l'Annexe B , "Installation sur des systèmes HP-UX, Solaris et Linux à l'aide d'outils natifs" à la page B-3.

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

REMARQUE Si vous installez le composant Interface utilisateur (interface graphique utilisateur ou interface de ligne de commande), il faut au préalable mettre à jour les variables d'environnement. Pour plus d'informations, reportez-vous à la section "Configuration des variables d'environnement" à la page 29.

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

Etape suivante

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

1. Si vous avez installé le Serveur d'installation sur un système autre que celui du Gestionnaire de cellule, il faut ajouter (importer) manuellement le système dans la cellule Data Protector. Reportez-vous à la section “Importation d'un Serveur d'installation dans une cellule” à la page 199.

REMARQUE

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

2. Installez le Serveur d'installation pour Windows si vous disposez de systèmes Windows dans votre cellule Data Protector. Reportez-vous à la section “Installation d'un Serveur d'installation pour Windows” à la page 44.
3. Distribuez le logiciel aux clients. Reportez-vous à la section “Installation des clients Data Protector” à la page 50.

Installation d'un Serveur d'installation pour Windows

Configuration système requise

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

- ✓ Disposer de l'une des versions du système d'exploitation Windows prises en charge. Reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector* pour connaître les versions de système d'exploitation prises en charge pour le Serveur d'installation.
- ✓ Disposer de Microsoft Internet Explorer 5.0 ou supérieur.
- ✓ Disposer d'un espace disque suffisant pour l'intégralité du dépôt de logiciel de Data Protector. Pour plus de détails à ce sujet, reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage Data Protector* .
- ✓ Avoir accès à un lecteur de DVD-ROM.
- ✓ Disposer de l'implémentation Microsoft du protocole TCP/IP, lequel doit être en cours d'exécution. Ce protocole doit pouvoir résoudre les noms d'hôte. Les noms de l'ordinateur et de l'hôte doivent être identiques. Reportez-vous à la section “Paramétrage du protocole TCP/IP sur les systèmes Windows” à la page B-21 pour obtenir des informations sur l'installation et la configuration du protocole TCP/IP.

Limites

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

Recommandation

Avant de procéder à l'installation de Data Protector A.06.00, assurez-vous que vous disposez de Microsoft Installer (MSI) 2.0. Si vous possédez une version plus ancienne de MSI, le programme d'installation de Data Protector va automatiquement le mettre à niveau avec la version 2.0. Dans ce cas, Data Protector affichera une remarque à la fin de l'installation, indiquant que MSI a été mis à niveau. Si MSI a été mis à niveau, il est vivement recommandé de redémarrer le système. Consultez le support de Microsoft pour en savoir plus sur les prérequis de MSI 2.0 en fonction des différents systèmes d'exploitation Windows.

Il est recommandé de mettre MSI à niveau vers la version 2.0 avant d'installer Data Protector A.06.00.

IMPORTANT

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

REMARQUE

Il est impossible d'installer à distance un client Data Protector sur le système Windows si un Serveur d'installation est déjà installé sur ce système. Pour installer un Serveur d'installation et un (des) composant(s) client sur le même système, vous devez procéder à une installation locale du client. Au cours de la procédure d'installation, sélectionnez tous les composants client de votre choix ainsi que le composant Serveur d'installation. Reportez-vous à la section "Installation de clients Windows" à la page 68.

Procédure d'installation

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

1. Insérez le DVD-ROM d'installation Windows et exécutez :

   Systèmes 32 bits : `\Windows_other\i386\setup.exe`

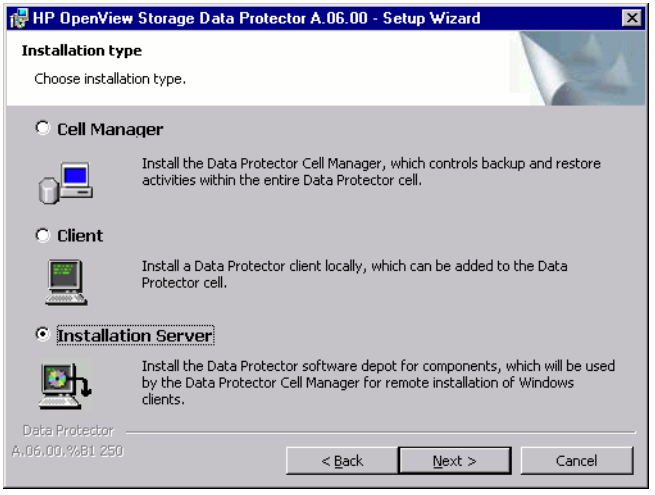
   Systèmes 64 bits : `\Windows_other\x8664\setup.exe`

   L'assistant d'installation de Data Protector s'affiche.

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

3. Dans la page `Type d'installation`, sélectionnez `Serveur d'installation`, puis cliquez sur `Suivant` pour installer le dépôt de logiciel Data Protector.

Figure 2-7 Sélection du type d'installation



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

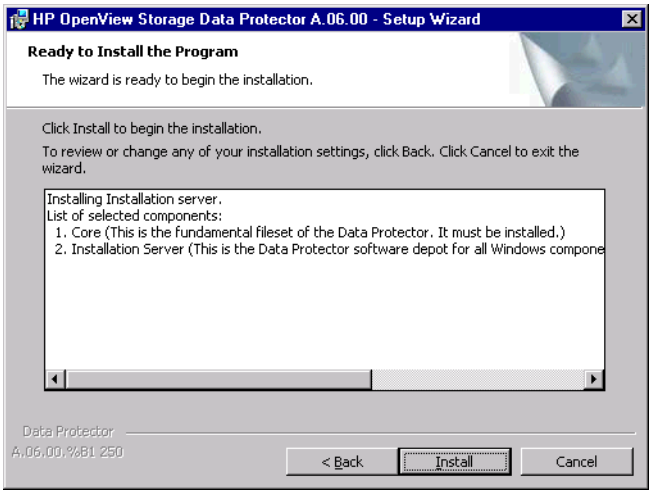
   Sinon, cliquez sur `Modifier` pour ouvrir la fenêtre `Modifier le dossier de destination actuel` et entrez un autre chemin.

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

   Cliquez sur `Suivant`.

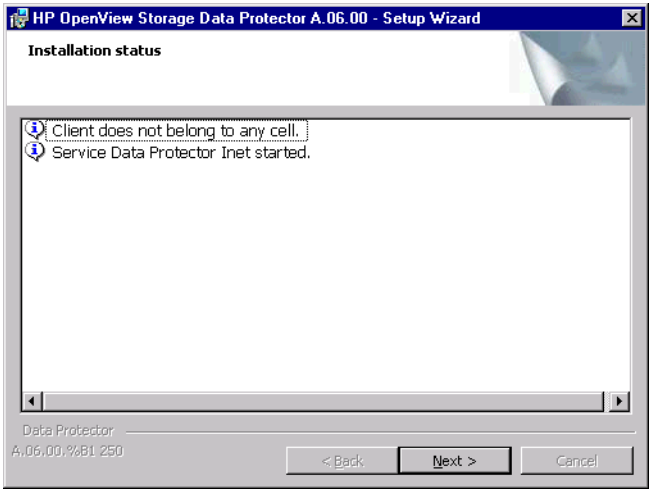
6. La liste des composants sélectionnés s'affiche. Cliquez sur `Installer` pour démarrer l'installation des composants sélectionnés. L'installation peut durer plusieurs minutes.

Figure 2-8 Page de résumé des composants sélectionnés



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

Figure 2-9 Page d'état de l'installation



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

   Cliquez sur `Terminer`.

Dès que l'installation est terminée, le logiciel est placé par défaut dans le répertoire *<répertoire_Data_Protector>*\Depot, lequel est partagé de sorte qu'il soit accessible par le réseau.

Etape suivante

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

1. Si vous avez configuré un Serveur d'installation indépendant (c'est-à-dire ne figurant pas dans le Gestionnaire de cellule), il faut ajouter (importer) manuellement le système dans la cellule Data Protector. Reportez-vous à la section “Importation d'un Serveur d'installation dans une cellule” à la page 199.

2. Installez un Serveur d'installation pour UNIX sous HP-UX, Solaris ou Linux, si votre environnement de sauvegarde est mixte. Reportez-vous à la section "Installation des Serveurs d'installation pour UNIX" à la page 40.
3. Distribuez le logiciel aux clients. Reportez-vous à la section "Installation des clients Data Protector" à la page 50.

Installation des clients Data Protector

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

Pour obtenir la liste des DVD-ROM d'installation de Data Protector, reportez-vous à la section “DVD-ROM d'installation de Data Protector” à la page 8.

Une fois que vous avez installé les clients Data Protector et, le cas échéant, les avez importés dans la cellule Data Protector, il est fortement recommandé de vérifier l'installation et de protéger les clients contre tout accès non autorisé. Pour connaître la procédure de vérification de l'installation du client, reportez-vous à la section “Vérification de l'installation du client Data Protector” à la page 357. Pour plus d'informations sur la sécurité, reportez-vous à la section “Considérations sur la sécurité” à la page 207.

Le tableau 2-1 répertorie les systèmes client Data Protector et contient des références permettant d'accéder à des descriptions détaillées.

Tableau 2-1 Installation des systèmes client Data Protector

Système client	Type d'installation et référence
Windows	Installation à distance et en local ; voir la section “Installation de clients Windows” à la page 68.
HP-UX	Installation à distance et en local ; voir la section “Installation de clients HP-UX” à la page 74.
AIX	Installation à distance et en local ; voir la section “Installation de clients AIX” à la page 92.
Solaris	Installation à distance et en local ; voir la section “Installation de clients Solaris” à la page 79.

Tableau 2-1 Installation des systèmes client Data Protector

Système client	Type d'installation et référence
Tru64	Installation à distance et en local ; voir la section “Installation de clients Tru64” à la page 97.
Siemens Sinix	Installation à distance et en local ; voir la section “Installation de clients Siemens Sinix” à la page 94.
SCO	Installation à distance et en local ; voir la section “Installation de clients SCO” à la page 99.
Linux	Installation à distance et en local ; voir la section “Installation de clients Linux” à la page 86.
Client DAS	Installation à distance et en local ; voir la section “Installation d'un Agent de support pour l'utilisation de la bibliothèque ADIC/GRAU ou StorageTek” à la page 102.
Client ACS	Installation à distance et en local ; voir la section “Installation d'un Agent de support pour l'utilisation de la bibliothèque ADIC/GRAU ou StorageTek” à la page 102.
Novell NetWare	Installation en local ; voir la section “Installation locale de clients Novell NetWare” à la page 112.
OpenVMS	Installation en local ; voir la section “Installation locale de clients OpenVMS” à la page 119.
MPE/iX	Installation en local ; voir la section “Installation de clients MPE/iX” à la page 127.

Tableau 2-1 Installation des systèmes client Data Protector

Système client	Type d'installation et référence
Autres clients UNIX	Installation en local ; voir la section “Installation locale de clients UNIX” à la page 130.

Intégrations

Les intégrations Data Protector sont des composants logiciels vous permettant de sauvegarder des applications de base de données avec Data Protector. Les systèmes exécutant ces applications s'installent de la même manière que tout système client Windows ou UNIX, à condition d'avoir sélectionné le composant logiciel approprié (par exemple, le composant `Intégration MS Exchange 2000/2003` pour la sauvegarde de la base de données Microsoft Exchange Server, le composant `Intégration Oracle` pour la sauvegarde de la base de données Oracle, etc.). Pour connaître les références, reportez-vous au tableau 2-2.

Tableau 2-2 Installation d'intégrations

Application	Référence
Microsoft Exchange Server	Voir “Clients Microsoft Exchange Server” à la page 139.
Microsoft SQL Server	Voir “Clients MS SQL” à la page 139.
Sybase	Voir “Clients Sybase” à la page 139.
Informix Server	Voir “Clients Informix Server” à la page 140.
SAP R/3	Voir “Clients SAP R/3” à la page 141.
SAP DB	Voir “Clients SAP DB” à la page 141.
Oracle	Voir “Clients Oracle” à la page 142.
IBM DB2 UDB	Voir “Clients DB2” à la page 143.
NNM	Voir “Clients NNM” à la page 143.
NDMP	Voir “Clients NDMP” à la page 143.
Microsoft Volume Shadow Copy	Voir “Clients Cliché instantané de volumes MS” à la page 144.

Tableau 2-2 Installation d'intégrations

Application	Référence
Lotus Domino Server	Voir “Clients Lotus Notes/Domino Server” à la page 144.
EMC Symmetrix	Voir “Intégration EMC Symmetrix” à la page 145.
HP StorageWorks XP	Voir “Intégration de HP StorageWorks XP” à la page 149.
HP StorageWorks Virtual Array	Voir “Intégration de HP StorageWorks Virtual Array” à la page 155.
HP StorageWorks Enterprise Virtual Array	Voir “Intégration de HP StorageWorks Enterprise Virtual Array” à la page 161.

Tableau 2-3 Autres installations

Installation	Référence
Interface utilisateur localisée	Voir “Installation de l'interface utilisateur localisée de Data Protector” à la page 168.
Rapports Web	Voir “Installation du composant Rapports Web de Data Protector” à la page 175.
MC/ServiceGuard	Voir “Installation de Data Protector sur MC/ServiceGuard” à la page 177.
Microsoft Cluster Server	Voir “Installation de Data Protector sur Microsoft Cluster Server” à la page 179.
Veritas Cluster Server	Voir “Installation de clients Data Protector sur un cluster Veritas” à la page 190.
Novell NetWare Cluster	Voir “Installation de clients Data Protector sur un cluster Novell NetWare” à la page 191.

Installation distante de clients Data Protector

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

Configuration système requise

- Pour connaître les conditions préalables et les recommandations d'installation, reportez-vous à la section décrivant la procédure d'installation pour ce client particulier. Les références sont énumérées dans le tableau 2-1 à la page 50 et le tableau 2-2 à la page 52.
- Pour obtenir la liste des plates-formes et des composants Data Protector pris en charge et connaître l'espace disque requis, reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le(s) Serveur(s) d'installation doivent être installés sur votre réseau.

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

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

- Pour utiliser une installation via un shell sécurisé, installez et configurez OpenSSH sur le client et le Serveur d'installation. Si votre clé privée est cryptée, installez et configurez Keychain sur le Serveur d'installation. Reportez-vous à la section "Installation à distance via un shell sécurisé" à la page 60 pour connaître la procédure de cette installation.

REMARQUE Vous ne pouvez pas distribuer le logiciel aux clients situés dans une autre cellule Data Protector. Toutefois, si vous disposez d'un Serveur d'installation indépendant, vous pouvez l'importer dans plusieurs

cellules. Vous pouvez ensuite distribuer le logiciel au sein de différentes cellules à l'aide de l'interface graphique utilisateur connectée à chaque Gestionnaire de cellule à tour de rôle.

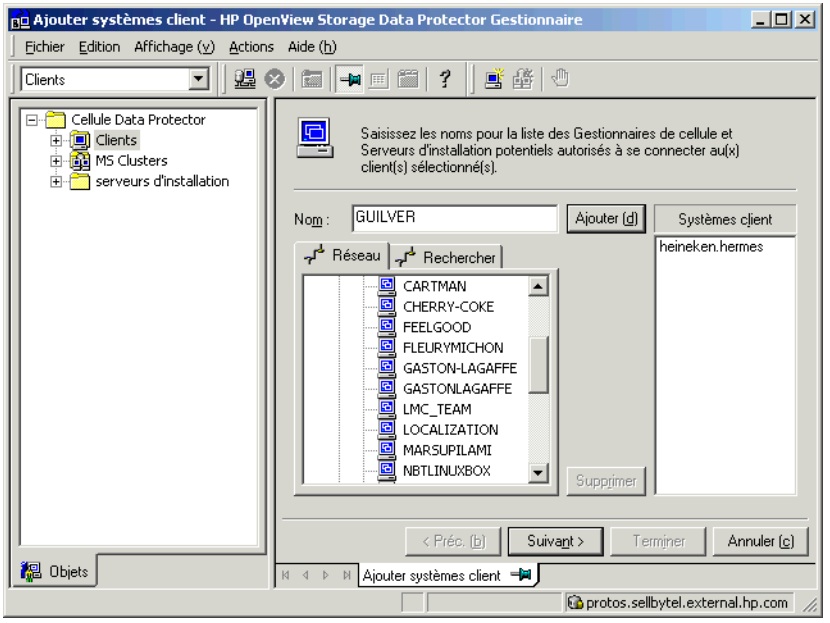
Ajout de clients à la cellule

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

1. Démarrez l'interface graphique utilisateur de Data Protector :
   - Sous Windows : sélectionnez `Démarrer->Programmes->HP OpenView Storage Data Protector->Gestionnaire Data Protector`.
   - Sur HP-UX ou Solaris : entrez `/opt/omni/bin/xomni` sur la ligne de commande.

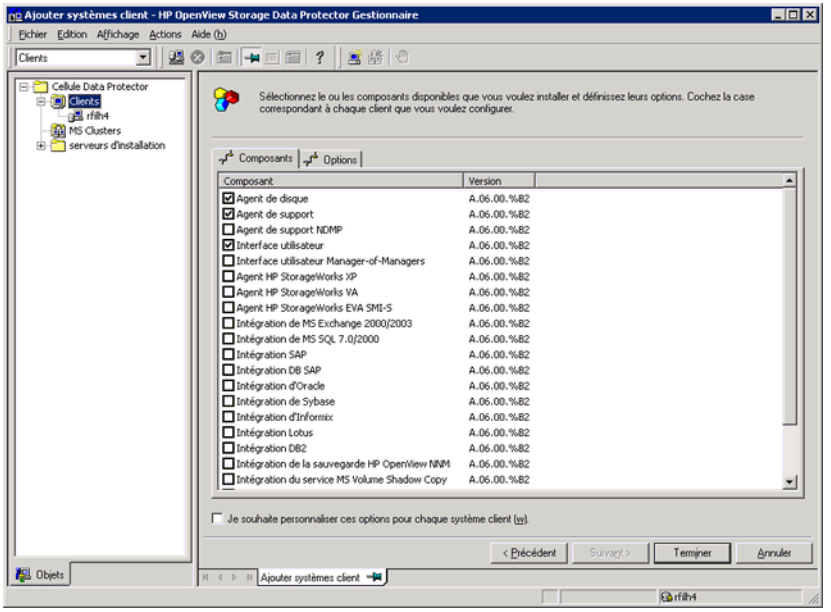
   Reportez-vous à l'aide en ligne pour plus de détails sur l'interface utilisateur graphique de Data Protector.
2. Dans le `Gestionnaire Data Protector`, cliquez sur `Clients`.
3. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur `Clients`, puis cliquez sur `Ajouter clients`.
4. Si plusieurs Serveurs d'installation sont configurés, sélectionnez la plate-forme des clients à installer (UNIX ou Windows) et le Serveur d'installation à utiliser pour la procédure. Cliquez sur `Suivant`.
5. Entrez les noms des clients ou recherchez les clients (interface Windows uniquement) à importer comme l'illustre la figure 2-10. Cliquez sur `Suivant`.

Figure 2-10 **Sélection de clients**



6. Sélectionnez les composants Data Protector à installer comme l'illustre la figure 2-11. Notez que vous ne pouvez sélectionner qu'un type d'Agent de support. Reportez-vous à la section “Composants Data Protector” à la page 63.

Figure 2-11 Sélection de composants



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

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

Cliquez sur `Terminer` pour démarrer l'installation.

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

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

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

Dépannage Dès que l'installation à distance est terminée, vous pouvez relancer les procédures d'installation qui ont échoué via l'interface en cliquant sur `Actions` et `Redémarrer clients ayant échoué`.
Si l'installation échoue de nouveau, reportez-vous à la section “Résolution des problèmes d'installation” à la page 345.

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

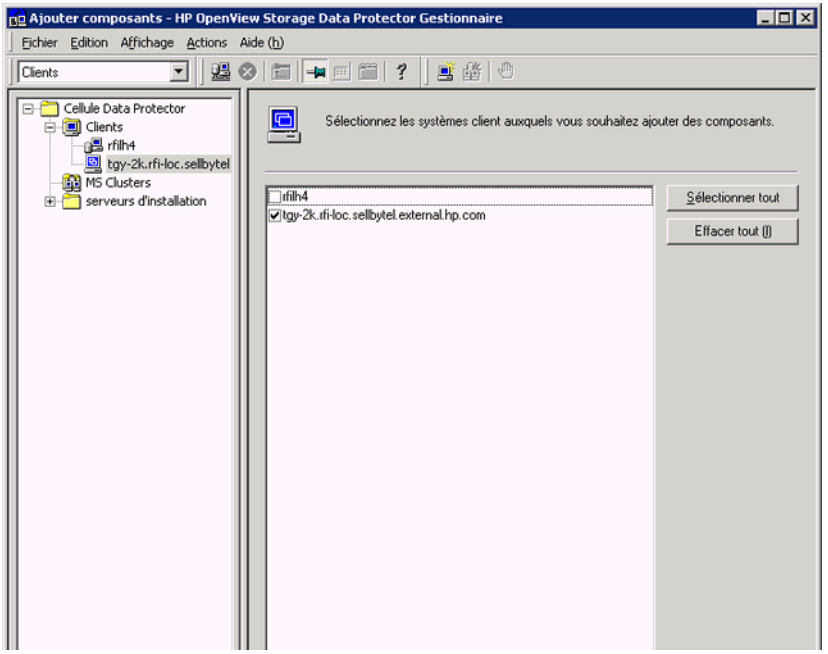
Clients MC/ServiceGuard Dans l'environnement de cluster MC/ServiceGuard, vérifiez que le nœud auquel vous ajoutez les composants est actif.

Condition préalable Le Serveur d’installation correspondant doit être disponible.

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

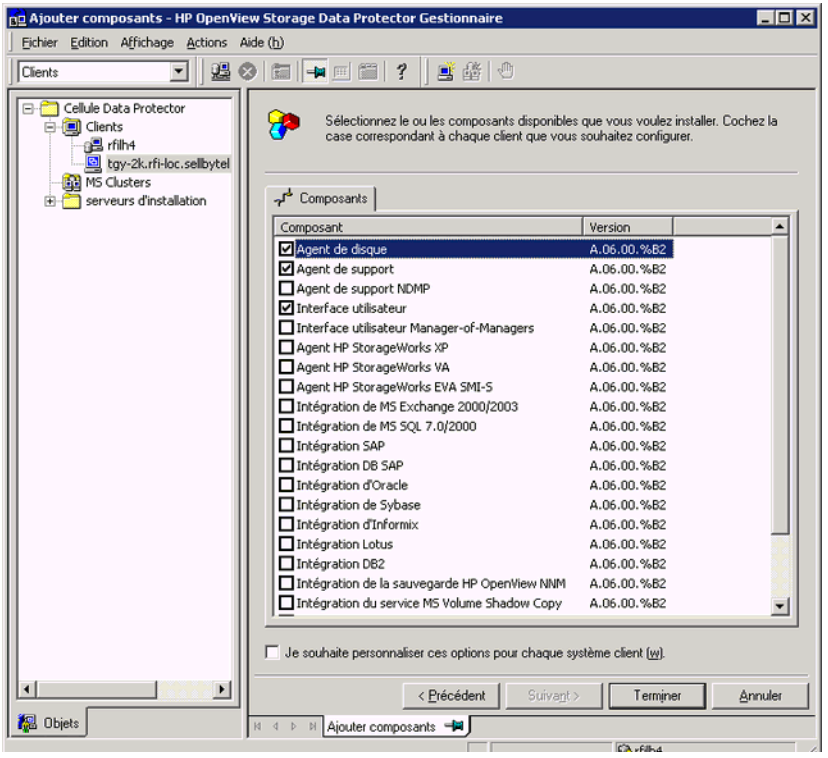
1. Dans le `Gestionnaire Data Protector`, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, développez `Clients`, cliquez avec le bouton droit de la souris sur un client, puis cliquez sur `Ajouter composants`.
3. Si plusieurs Serveurs d'installation sont configurés, sélectionnez la plate-forme des clients sur lesquels installer les composants (UNIX ou Windows) et le Serveur d’installation à utiliser pour la procédure. Cliquez sur `Suivant`.
4. Sélectionnez les clients sur lesquels vous souhaitez installer les composants comme illustré dans la figure 2-12. Cliquez sur `Suivant`.

Figure 2-12 Sélection de clients



5. Sélectionnez les composants Data Protector à installer comme l'illustre la figure 2-13. Notez que vous ne pouvez sélectionner qu'un type d'Agent de support. Reportez-vous à la section “Composants Data Protector” à la page 63.

Figure 2-13 **Sélection de composants**



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

Cliquez sur `Terminer` pour démarrer l'installation.

Installation à distance via un shell sécurisé

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

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

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

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

Configuration de OpenSSH

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

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

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

2. Sur le Serveur d'installation, exécutez `ssh-keygen` pour générer une paire de clés publique-privée. Conservez la clé privée sur le Serveur d'installation et transférez la clé publique sur le client. Notez que si vous utilisez une clé privée cryptée (c'est-à-dire, protégée par une phrase passe), vous devez configurer Keychain sur le Serveur d'installation (voir la page 62 pour plus de détails).

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

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

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

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

a. ***Sur le Serveur d'installation :***

`<répertoire_installation_ssh>/ssh/etc/ssh_config`

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

b. ***Sur le client :***

`<répertoire_installation_ssh>/ssh/etc/sshd_config`

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

Notez que ces deux fichiers doivent être synchronisés.

REMARQUE La version de protocole SSH par défaut est SSH2.

4. Sur le client, démarrez le démon `ssh` :

   `<répertoire_installation_ssh>/ssh/sbin/sshd`

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

   `ssh root@<hôte_client>`

   Notez que `<hôte_client>` doit être le nom DNS complet, par exemple :

   `ssh root@client1.société.com`

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

Configuration de Keychain

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

1. Téléchargez Keychain à l'adresse http://www.gentoo.org/proj/en/keychain/index.xml vers le Serveur d'installation.
2. Ajoutez au fichier `$HOME/.profile` les deux lignes suivantes :

HP-UX, Solaris :

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

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

Linux :

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

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

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

Etape suivante

Après avoir configuré OpenSSH et Keychain, ajoutez des clients à la cellule à l'aide de l'interface graphique comme décrit à la page 55 ou à l'aide de l'interface de ligne de commande en exécutant la commande ob2install. Pour plus d'informations sur les commandes de l'interface de ligne de commande et leurs paramètres, reportez-vous à la *Référence de l'interface de ligne de commande HP OpenView Storage Data Protector*.

REMARQUE

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

Composants Data Protector

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

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

Interface utilisateur	L'interface utilisateur comprend l'interface graphique utilisateur Data Protector et l'interface de ligne de commande. Ce logiciel est nécessaire

	pour accéder au Gestionnaire de cellule Data Protector et doit être installé au moins sur le système utilisé pour gérer la cellule.

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

Interface utilisateur Manager-of-Managers (MoM)	L'interface utilisateur Manager-of-Managers (MoM) comprend l'interface graphique utilisateur de Data Protector et l'interface de ligne de commande. Ce logiciel est nécessaire pour accéder aux fonctionnalités Manager-of-Managers de Data Protector et pour contrôler l'environnement multicellules.
Agent de disque	Le composant Agent de disque doit être installé sur les clients disposant de disques qui doivent être sauvegardés avec Data Protector.
Agent général de supports	Le composant Agent général de supports doit être installé sur les clients auxquels sont reliés des périphériques de sauvegarde ou qui disposent d'un accès au robot de bibliothèque et qui seront gérés avec Data Protector.
Récupération après sinistre automatique	Le composant Récupération après sinistre automatique doit être installé sur les clients pour lesquels vous souhaitez activer la récupération à l'aide d'une méthode

	automatique de récupération après sinistre et sur le système sur lequel l'image CD ISO DR pour la récupération après sinistre avancée sera préparée, afin de fournir une préparation automatique en vue de la récupération après sinistre avancée.
Intégration SAP R/3	Le composant Intégration SAP R/3 doit être installé sur les clients disposant d'une base de données SAP R/3 qui sera sauvegardée avec Data Protector.
Intégration SAP DB	Le composant Intégration SAP DB doit être installé sur les clients disposant d'une base de données SAP DB qui sera sauvegardée avec Data Protector.
Intégration Oracle	Le composant Intégration Oracle doit être installé sur les clients disposant d'une base de données Oracle qui sera sauvegardée avec Data Protector.
Intégration DB2	Le composant Intégration DB2 doit être installé sur tous les clients disposant d'un serveur DB2 qui sera sauvegardé avec Data Protector.
Intégration Sybase	Le composant Intégration Sybase doit être installé sur les clients disposant d'une base de données Sybase qui sera sauvegardée avec Data Protector.
Intégration Informix	Le composant Intégration Informix doit être installé sur les clients disposant d'une base de données Informix Server qui sera sauvegardée avec Data Protector.
Intégration MS Exchange 2000/2003	Le composant Intégration MS Exchange 2000/2003 doit être installé sur les clients disposant d'une base

	de données Microsoft Exchange Server qui sera sauvegardée avec Data Protector.
Intégration MS SQL 7.0/2000	Le composant Intégration SQL 7.0/2000 doit être installé sur les systèmes où une base de données MS SQL sera sauvegardée avec Data Protector.
Intégration du service MS Volume Shadow Copy	Le composant Intégration du service MS Volume Shadow Copy doit être installé sur les systèmes Windows Server 2003 sur lesquels vous souhaitez exécuter des sauvegardes coordonnées par le service Volume Shadow Copy.
Agent EMC Symmetrix	Le composant Agent EMC Symmetrix doit être installé sur le système d'application et de sauvegarde pour intégrer EMC Symmetrix dans Data Protector.
Agent HP StorageWorks XP	Le composant Agent HP StorageWorks XP doit être installé sur le système d'application et de sauvegarde pour intégrer HP StorageWorks XP dans Data Protector.
Agent HP StorageWorks VA	Le composant Agent HP StorageWorks VA doit être installé sur le système d'application et de sauvegarde pour intégrer HP StorageWorks Virtual Array dans Data Protector.
Agent HP StorageWorks EVA SMI-S	Le composant Agent HP StorageWorks EVA SMI-S doit être installé sur le système d'application

	et de sauvegarde pour intégrer HP StorageWorks Enterprise Virtual Array dans Data Protector.
Cluster Server	Le composant Cluster Server doit être installé sur tous les clients Data Protector compatibles cluster.
Intégration HP OpenView NNM	Le composant Intégration NNM doit être installé sur tous les clients de la cellule où réside la base de données NNM devant être sauvegardée avec Data Protector.
Agent de support NDMP	L'Agent de support NDMP doit être installé sur tous les systèmes clients qui sauvegardent des données vers des lecteurs dédiés NDMP via un serveur NDMP.
Intégration Lotus	Le composant Intégration Lotus doit être installé sur tous les clients de la cellule où réside une base de données Lotus Notes/Domino Server qui sera sauvegardée avec Data Protector.
Support de langue français	Le composant Support de langue français doit être installé sur des clients sur lesquels vous souhaitez utiliser l'Interface utilisateur de Data Protector localisée en français.
Support de langue japonais	Le composant Support de langue japonais doit être installé sur des clients sur lesquels vous souhaitez utiliser l'Interface utilisateur de Data Protector localisée en japonais.

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

Installation de clients Windows

Pour obtenir des informations plus détaillées sur les plates-formes et les composants pris en charge pour un système d'exploitation Windows particulier, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

Configuration système requise

Pour installer un client Windows, vous devez utiliser le compte Administrateur. Le système Windows qui deviendra votre système client Data Protector doit répondre aux critères suivants :

- ✓ Disposer de Microsoft Internet Explorer 5.0 ou supérieur.
- ✓ Disposer d'un espace disque suffisant pour le logiciel client Data Protector. Pour plus de détails à ce sujet, reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage Data Protector* .
- ✓ Disposer du port numéro 5555 (par défaut).
- ✓ Disposer de l'implémentation Microsoft du protocole TCP/IP, lequel doit être installé et en cours d'exécution. Ce protocole doit pouvoir résoudre les noms d'hôte. Les noms de l'ordinateur et de l'hôte doivent être identiques. Reportez-vous à la section “Paramétrage du protocole TCP/IP sur les systèmes Windows” à la page B-21 pour obtenir des informations sur l'installation et la configuration du protocole TCP/IP.

Limites

- En raison des restrictions de sécurité imposées par le système d'exploitation Windows, le Serveur d’installation peut être utilisé pour installer des clients à distance uniquement dans le même domaine.
- Sous Windows Me/XP Edition familiale, les clients Data Protector peuvent uniquement être installés en local.

Recommandation

Sur chaque client Windows, assurez-vous que vous disposez de Microsoft Installer (MSI) 2.0 avant d'installer Data Protector A.06.00. Si vous possédez une version plus ancienne de MSI, le programme d'installation de Data Protector va automatiquement le mettre à niveau avec la version 2.0. Dans ce cas, Data Protector affichera une remarque à la fin de l'installation, indiquant que MSI a été mis à niveau. Si MSI a été mis à niveau, il est vivement recommandé de redémarrer le système client.

Consultez le support technique Microsoft pour connaître la configuration requise pour Microsoft Installer 2.0 sur les différents systèmes d'exploitation Windows.

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

Récupération après sinistre automatique

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

Clients compatibles cluster

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

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section “Composants Data Protector” à la page 63.

Installation en local

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

1. Insérez le DVD-ROM et exécutez la commande :

   Systèmes à processeur 32 bits : `\Windows_other\i386\setup.exe`

   Systèmes à processeur AMD-64/Intel EM64T : `\Windows_other\x8664\setup.exe`

   Systèmes à processeur Itanium : `\Windows_other\ia64\setup.exe`.

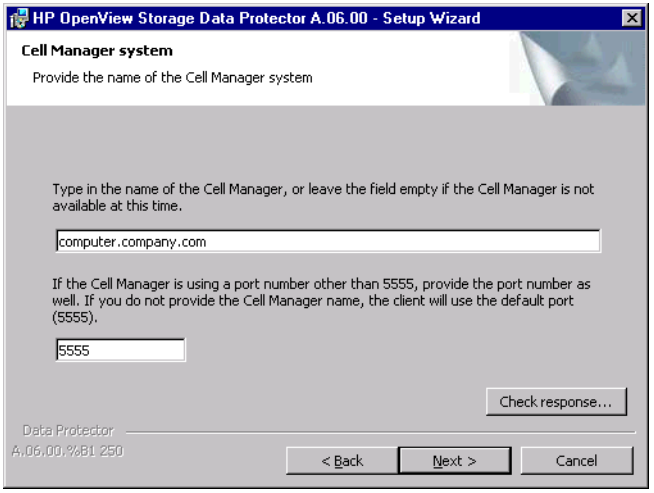
2. Dans la page `Type d'installation`, sélectionnez `Client`. Pour les clients Itanium, le type est sélectionné automatiquement.

3. Saisissez le nom du Gestionnaire de cellule. Reportez-vous à la figure 2-14.

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

Cliquez sur `Suivant`.

Figure 2-14 Choix du Gestionnaire de cellule



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

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

5. Sélectionnez les composants de Data Protector à installer.

   Pour obtenir des informations sur les composants Data Protector, reportez-vous à la section “Composants Data Protector” à la page 63.

   Cliquez sur `Suivant`.

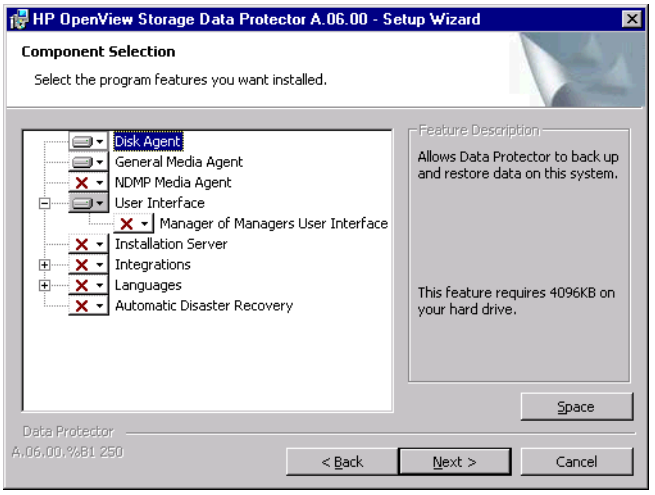
6. ***Windows XP SP2, Windows 2003 SP1 :*** si Data Protector détecte le pare-feu Windows sur votre système, la page Configuration du pare-feu Windows est affichée. Data Protector enregistrera tous les exécutables Data Protector nécessaires. Par défaut, l'option `Permettre initialement aux nouveaux fichiers binaires Data Protector enregistrés d'ouvrir des ports le cas`

échéant est sélectionnée. Si vous ne souhaitez pas activer Data Protector pour les ports ouverts, désélectionnez l'option. Toutefois, notez que les exécutables doivent être activés pour que Data Protector fonctionne correctement.

Cliquez sur Suivant.

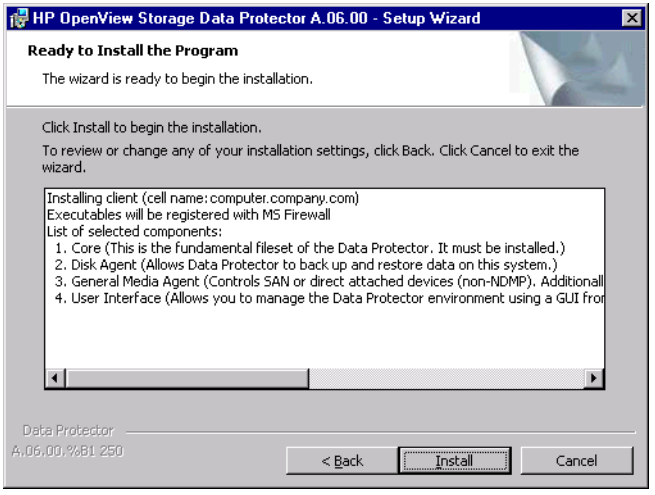
7. La liste des composants sélectionnés s'affiche. Cliquez sur Installer pour installer les composants sélectionnés.

Figure 2-15 Page de résumé des composants sélectionnés



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

Figure 2-16 Page de résumé de l'installation



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

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

   Cliquez sur `Terminer`.

Connexion d'un périphérique de sauvegarde aux systèmes Windows

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

1. Recherchez les adresses SCSI disponibles (désignées sous le nom de *ID SCSI cibles* sous Windows) pour les lecteurs et le périphérique de contrôle (robot) du périphérique de sauvegarde à connecter. Reportez-vous à la section “Recherche des ID SCSI cibles inutilisés sur un système Windows” à la page B-59.

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

   Pour plus d'informations sur les périphériques pris en charge, reportez-vous également à l'adresse : http://www.hp.com/support/manuals.

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

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

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

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

   - Si le pilote de bandes de votre périphérique est chargé :

     ```
     HP:C1533A

     tape3:0:4:0

     DDS

     ...
     ```

     La première ligne représente la spécification du périphérique, la seconde indique le nom du fichier du périphérique.

     Le format du chemin d'accès indique qu'un périphérique à bande HP DDS est doté du numéro d'instance de lecteur 3 et est connecté au bus SCSI 0, à l'ID SCSI cible 4 et au LUN numéro 0.

   - Si le pilote de bandes de votre périphérique n'est pas chargé :

     ```
     HP:C1533A

     scsi1:0:4:0

     DDS

     ...
     ```

La première ligne représente la spécification du périphérique, la seconde indique le nom du fichier du périphérique.

Le format du chemin d'accès indique qu'un périphérique à bande HP DDS est relié au port SCSI 1 et au bus SCSI 0, et que le lecteur de bande possède l'ID SCSI cible 4 et le numéro de LUN 0.

Pour charger ou décharger le pilote de bandes d'origine de votre périphérique, reportez-vous à la section “Utilisation de pilotes de bandes et de pilotes de robots sous Windows” à la page B-34. Pour plus d'informations sur la création d'un fichier de périphérique, reportez-vous à la section “Création de fichiers de périphérique (adresses SCSI) sous Windows” à la page B-38.

Etape suivante

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

Installation de clients HP-UX

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

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section “Composants Data Protector” à la page 63.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes, processeurs et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d’installation pour UNIX doivent être installés sur votre réseau. Le cas échéant, reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d’installation (IS) de Data Protector” à la page 19 pour obtenir des instructions.
- Pour installer un client HP-UX, vous devez disposer soit d'un accès *root*, soit d'un compte doté des droits *root*.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section “Installation locale de clients UNIX” à la page 130 pour de plus amples informations.

Après l'installation en local, le système client doit être importé manuellement dans la cellule. Reportez-vous également à la section “Importation de clients dans une cellule” à la page 197.

Installation à distance

Vous devez installer le logiciel client à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur de Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section “Installation distante de clients Data Protector” à la page 54.

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

Si vous avez installé un Agent de support sur le système client, vous devez connecter physiquement le périphérique de sauvegarde au système. Pour savoir si les pilotes de périphériques correspondant au type de votre périphérique sont déjà intégrés dans le noyau, vérifiez la configuration du noyau avant d'exécuter une sauvegarde.

Clients compatibles cluster

D'autres conditions et étapes sont requises pour l'installation de clients compatibles cluster. Pour plus de détails, reportez-vous à la section “Installation d'un client compatible cluster” à la page 178.

Vérification de la configuration du noyau sous HP-UX

La procédure suivante explique comment vérifier et déterminer la configuration de votre noyau sur le système HP-UX 11.x à l'aide de l'utilitaire *HP System Administration Manager (SAM)*. Pour connaître la procédure manuelle de création du noyau, reportez-vous à la section “Configuration de robot SCSI sous HP-UX” à la page B-41.

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

1. Connectez-vous comme utilisateur `root`, ouvrez le terminal puis tapez `sam`.
2. Dans la fenêtre `System Administration Manager`, cliquez deux fois sur `Configuration du kernel`, puis cliquez sur `Pilotes`.

3. Dans la fenêtre `Configuration du kernel`, vérifiez les éléments suivants :

   ✓ Les pilotes des périphériques que vous allez utiliser doivent apparaître dans la liste des pilotes installés. Reportez-vous à la figure 2-17. Si le pilote que vous recherchez n'est pas mentionné, vous devez l'installer à l'aide de l'utilitaire `/usr/sbin/swinstall`. Par exemple :

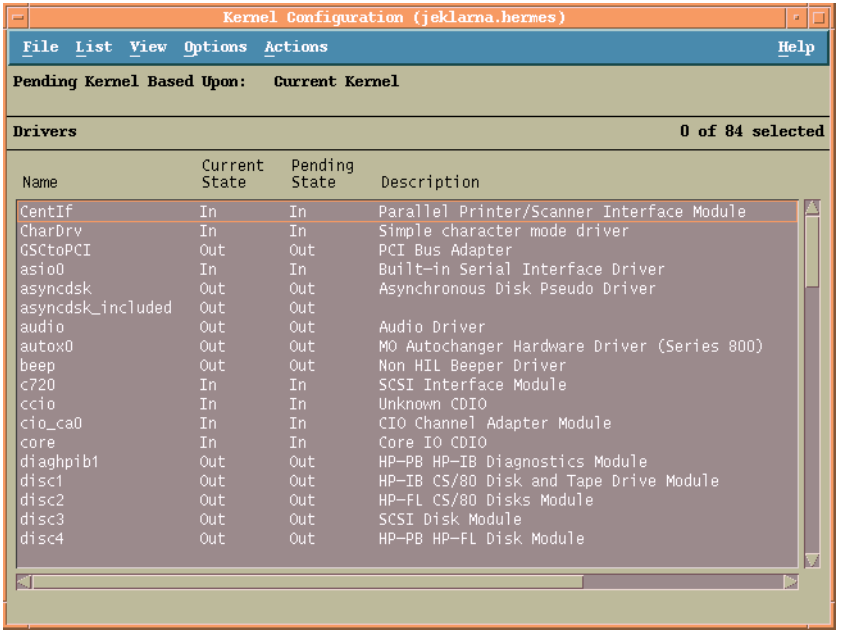
   - Un pilote de périphériques à bandes est requis pour les périphériques à bande et doit être installé si vous souhaitez connecter ce type de périphérique au système. Par exemple, le pilote `stape` est utilisé pour les lecteurs de bande SCSI génériques de type DLT ou LTO, alors que le pilote `tape2` est réservé aux périphériques DDS.

     Si vous avez connecté un périphérique Quantum DLT 4000 à un système HP-UX 11.00, nous vous recommandons d'utiliser le pilote `tape2` plutôt que `stape`.

   - Un pilote de passage SCSI nommé `sctl` ou `spt`, ou un pilote de robot de changeur automatique nommé `schgr` (selon le matériel) est requis pour contrôler le robot des périphériques de bibliothèque de bande.

     Pour obtenir des informations détaillées, reportez-vous à la section “Configuration de robot SCSI sous HP-UX” à la page B-41.

Figure 2-17 Fenêtre de configuration du kernel



✓ L'état d'un pilote affiché dans la colonne `Etat actuel` doit être défini à `Dedans`. Si la valeur de l'état est `Dehors`, procédez comme suit :

a. Sélectionnez le pilote dans la liste. Cliquez sur `Actions` et sélectionnez `Ajouter pilote au kernel`. L'état est alors réglé sur `Dedans` dans la colonne `Etat en attente`.

   Répétez cette étape pour chaque pilote dont l'`Etat actuel` est défini sur `Dedans`.

b. Cliquez sur `Actions` et sélectionnez `Créer kernel` pour appliquer les modifications, c'est-à-dire créer un `kernel en attente` dans le `kernel en cours`. Cette opération nécessite un redémarrage du système.

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

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

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

   Pour plus d'informations, reportez-vous à la section “Recherche des adresses SCSI non utilisées sous HP-UX” à la page B-50.

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

   Pour obtenir des informations détaillées sur les périphériques pris en charge, reportez-vous à la page http://www.hp.com/support/manuals.

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

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

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

   de manière à pouvoir visualiser la liste des fichiers de chaque périphérique de sauvegarde connecté. Si un fichier de périphérique n'a pas été créé automatiquement durant le processus d'amorçage, vous devez le créer manuellement. Reportez-vous à la section “Création de fichiers de périphérique sous HP-UX” à la page B-46.

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

Installation de clients Solaris

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

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section “Composants Data Protector” à la page 63.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector” à la page 19 pour obtenir des instructions.
- Pour installer un client Solaris, vous devez disposer soit d'un accès *root*, soit d'un compte doté des droits *root*.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section “Installation locale de clients UNIX” à la page 130 pour obtenir des instructions.

Installation à distance

Vous devez installer le logiciel client à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section “Installation distante de clients Data Protector” à la page 54.

REMARQUE Si vous installez le composant `Interface utilisateur` (comprenant l'interface graphique utilisateur et l'interface de ligne de commande), il faut au préalable mettre à jour les variables de votre environnement. Pour plus d'informations, reportez-vous à la section “Configuration des variables d'environnement” à la page 29.

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

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

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

`/opt/omni/ -> /<préfixe>/opt/omni/`

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

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

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

Clients compatibles cluster D'autres conditions sont requises pour l'installation de clients compatibles cluster. Pour plus de détails, reportez-vous à la section “Installation d'un client” à la page 190.

Configuration post-installation

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

- Pour un périphérique Exabyte (8 mm), aucune modification du fichier `/kernel/drv/st.conf` n'est requise.

- Pour un périphérique HP DAT (4 mm), ajoutez les lignes suivantes au fichier `/kernel/drv/st.conf` :

```
tape-config-list =

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

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

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

```
tape-config-list =

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

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

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

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

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

REMARQUE

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

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

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

  Pour installer le pilote de passage SCSI, procédez comme suit :

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

     Systèmes Solaris 32 bits :

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

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

Systèmes Solaris 64 bits :

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

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

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

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

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

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

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

```
add_drv sst
```

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

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

```
shutdown -i0
```

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

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

   Lorsque vous avez terminé, relancez le système avec :

```
ok boot -r
```

Pour installer le périphérique SCSI, procédez comme suit :

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

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

Exemple

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

   Les données de l'exemple ci-dessus doivent se trouver dans le fichier `/kernel/drv/st.conf`.

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

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

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

Connexion d'un périphérique de sauvegarde à un système Solaris

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

1. Créez un fichier `reconfigure` :

   ```
   touch /reconfigure
   ```

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

   Pour obtenir des informations détaillées sur les périphériques pris en charge, reportez-vous à la page http://www.hp.com/support/manuals.

REMARQUE

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

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

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

   puis entrez :

   ```
   ok > go
   ```

   pour continuer.

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

REMARQUE

Sur les systèmes Solaris (en particulier dans le cas de Solaris 64 bits), les liens vers le périphérique de contrôle SCSI (sélectionneur) ne sont pas toujours créés automatiquement. Dans ce cas, créez des liens symboliques. Par exemple :

```
ln -s /devices/pci@1f,4000/scsi@3,1/sst@4,1:character
/dev/rsst4
```

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

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

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

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

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

Etape suivante

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

Installation de clients Linux

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

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section “Composants Data Protector” à la page 63.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 19 pour de plus amples informations.
- L'utilitaire `rpm` doit être installé et configuré. Les autres systèmes de gestion de packages (tels que `deb`) ne sont pas pris en charge.

REMARQUE

L'interface graphique n'est pas prise en charge sous Linux. Toutefois, vous pouvez utiliser la commande `omniusers` pour créer un compte utilisateur distant sur le nouveau Gestionnaire de cellule. Vous pouvez alors utiliser ce compte utilisateur avec l'interface graphique utilisateur de Data Protector installée pour lancer l'interface et vous connecter au nouveau Gestionnaire de cellule. Reportez-vous à la page `omniusers` du manuel.

REMARQUE

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

Si ce numéro de port est déjà utilisé, vous devez le rendre disponible pour Data Protector ou remplacer cette valeur par défaut par le numéro d'un port non utilisé. Reportez-vous à la section "Modification du numéro de port par défaut" à la page B-30.

HP Cluster ServiceGuard

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

Une fois l'installation terminée, vous devez importer l'*hôte virtuel* (package d'application) dans la cellule sous forme de client. Le package d'application (par exemple Oracle) doit donc fonctionner sur le cluster avec son *adresse IP de serveur virtuel*. Utilisez la commande `cmviewcl -v` pour le vérifier avant d'importer le client.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section “Installation locale de clients UNIX” à la page 130 pour de plus amples informations.

Installation à distance

Vous pouvez installer à distance un système client Linux en distribuant les composants Data Protector à partir du Serveur d'installation pour UNIX sur le système Linux, à l'aide de l'interface graphique utilisateur de Data Protector. Pour connaître la procédure détaillée de cette opération, reportez-vous à la section “Installation distante de clients Data Protector” à la page 54.

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

Résolution des problèmes

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

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

   ```
   server_args = -h
   ```

   Par exemple :

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

   service exec
   {
   socket_type = stream
   protocol = tcp
   wait = no
   user = root
   ```

```
server = /usr/sbin/in.rexecd
server_args = -h
}
```

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

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

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

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

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

Pour obtenir plus d'informations, reportez-vous à la page du manuel `rexecd`(8), `rexec`(3), `rshd`(8), `rsh`(1) ou `pam`(8). En cas d'échec, reportez-vous à la section “Installation locale de clients UNIX” à la page 130.

Configuration du noyau

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

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

Si ces éléments sont déjà inclus dans le noyau, quittez le programme sans enregistrer les modifications. Vous pouvez poursuivre en connectant un périphérique de sauvegarde à votre système. Reportez-vous à la section “Connexion d'un périphérique de sauvegarde à un système Linux” à la page 91.

3. Si vous effectuez des modifications, enregistrez la configuration et procédez comme suit :

   a. Exécutez la commande `make dep`.

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

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

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

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

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

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

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

   ```
   image = /boot/newkernel

   label = new

   read-only
   ```

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

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

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

Connexion d'un périphérique de sauvegarde à un système Linux

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

1. Exécutez la commande `cat /proc/scsi/scsi` pour déterminer les adresses SCSI disponibles pour les lecteurs et le périphérique de contrôle (robot).
2. Définissez l'adresse SCSI sur le périphérique. En fonction du type de périphérique, vous pouvez effectuer cette opération à l'aide des commutateurs du périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

   Pour obtenir des informations détaillées sur les périphériques pris en charge, reportez-vous à la page http://www.hp.com/support/manuals.
3. Connectez le périphérique au système, allumez le périphérique, puis l'ordinateur et attendez que le processus d'amorçage soit terminé. Les fichiers du périphérique sont créés au cours de ce processus. (Sur RedHat Linux, une application, Kudzu, est lancée lors du processus d'amorçage lorsqu'un nouveau périphérique est connecté au système. Appuyez sur n'importe quelle touche pour lancer l'application, puis cliquez sur le bouton `Configurer`).
4. Pour vous assurer que le système reconnaît votre nouveau périphérique de sauvegarde, exécutez la commande `cat /proc/scsi/scsi`, puis la commande `dmesg |grep scsi`. Les fichiers du périphérique sont répertoriés pour chaque périphérique de sauvegarde connecté.

Exemples

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

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

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

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

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

   ```
   ll /dev | grep <fichier_périphérique>
   ```

   Par exemple :

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

   Le résultat de cette commande est le suivant :

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

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

Etape suivante

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

Installation de clients AIX

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

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section “Composants Data Protector” à la page 63.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 19 pour obtenir des instructions.

IMPORTANT

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

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

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

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section "Installation locale de clients UNIX" à la page 130 pour obtenir des instructions.

Installation à distance

Vous devez installer le logiciel client AIX à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur de Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section "Installation distante de clients Data Protector" à la page 54.

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

Connexion d'un périphérique de sauvegarde à un client AIX

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

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

Pour obtenir des informations détaillées sur les périphériques pris en charge, reportez-vous à la page http://www.hp.com/support/manuals.

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

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

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

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

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

Installation de clients Siemens Sinix

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

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section “Composants Data Protector” à la page 63.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 19 pour de plus amples informations.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section "Installation locale de clients UNIX" à la page 130 pour de plus amples informations.

Installation à distance

Vous devez installer le logiciel client Sinix à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section "Installation distante de clients Data Protector" à la page 54.

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

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

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

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

   Pour plus d'informations sur les périphériques pris en charge et la documentation qui les accompagne, reportez-vous à la page Web http://www.hp.com/support/manuals.

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

2. Rallumez l'ordinateur et attendez que le processus d'amorçage soit terminé.
3. Sélectionnez le fichier de périphérique approprié dans le répertoire `/dev`.

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

REMARQUE

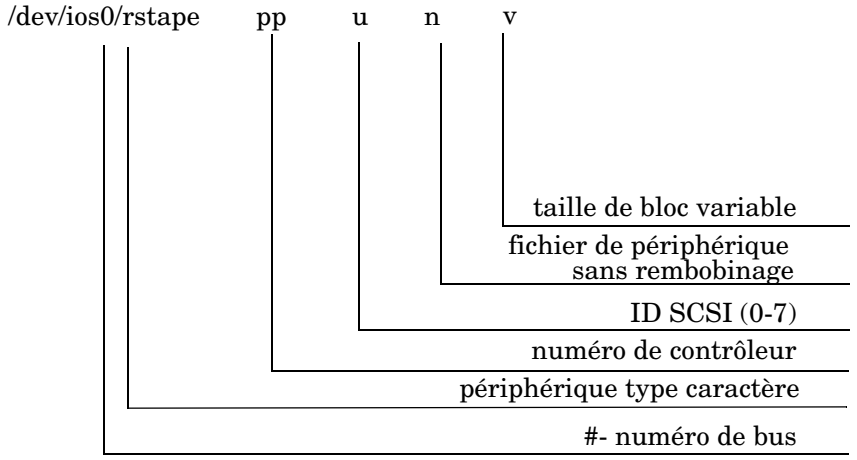
Les fichiers de périphérique spéciaux se trouvent dans le répertoire `/dev`. Vous devez donc ajouter le chemin d'accès `/dev` devant le nom du périphérique.

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

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

Le nom de fichier de périphérique `/dev/ios0/rstape006nv` est expliqué à la figure 2-18.

Figure 2-18 **Format de nom de fichier de périphérique :**



Etape suivante

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

Installation de clients Tru64

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

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section “Composants Data Protector” à la page 63.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 19 pour de plus amples informations.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section "Installation locale de clients UNIX" à la page 130 pour de plus amples informations.

Installation à distance

Vous devez installer le logiciel client Tru64 à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section "Installation distante de clients Data Protector" à la page 54.

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

Cluster Tru64

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

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

Après l'installation, il faut importer le nom d'hôte virtuel du cluster et les différents nœuds dans la cellule Data Protector. Pour connaître la procédure, reportez-vous à la section "Importation d'un client compatible dans une cellule" à la page 200

Connexion d'un périphérique de sauvegarde à un client Tru64

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

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

REMARQUE

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

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

Pour obtenir des informations détaillées sur les périphériques pris en charge, reportez-vous à la page http://www.hp.com/support/manuals.

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

Etape suivante

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

Installation de clients SCO

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

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

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section “Composants Data Protector” à la page 63.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector” à la page 19 pour de plus amples informations.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour UNIX. Reportez-vous à la section “Installation locale de clients UNIX” à la page 130 pour de plus amples informations.

Installation à distance

Vous devez installer le logiciel client SCO à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur de Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section “Installation distante de clients Data Protector” à la page 54.

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

Connexion d'un périphérique de sauvegarde à un système SCO

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

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

   Pour plus d'informations sur les périphériques pris en charge et la documentation qui les accompagne, reportez-vous à la page Web http://www.hp.com/support/manuals/

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

REMARQUE

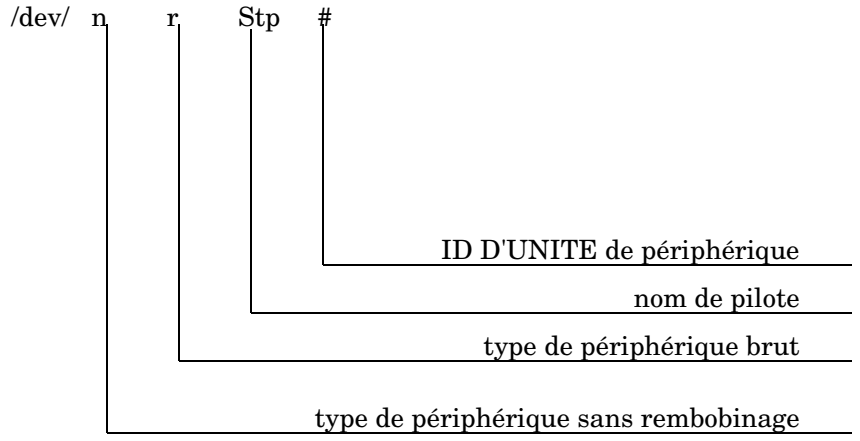
Notez l'ID d'unité, qui s'affiche lorsque vous exécutez la commande `mkdev tape`. Vous en aurez besoin pour reconnaître le nom de fichier du périphérique.

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

   Utilisez le nom `nrStp#`, dans lequel # représente l'ID D'UNITE du périphérique. L'ID D'UNITE du périphérique est définie à l'étape 4. Le nom de fichier de périphérique `/dev/nrStp#` est expliqué à la figure 2-19.

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

Figure 2-19 Format de nom de fichier de périphérique :



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

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

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

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

REMARQUE Vous devez disposer de licences spéciales, qui sont fonction du nombre de lecteurs et d'emplacements utilisés dans la bibliothèque StorageTek. Pour plus d'informations, reportez-vous au Chapitre 5, “Attribution de licences Data Protector”, page 315.

Connexion de lecteurs de bibliothèque

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

Pour plus d'informations sur les bibliothèques ADIC/GRAU ou STK prises en charge, reportez-vous à la page Web http://www.hp.com/support/manuals.

Reportez-vous à la section “Installation de clients HP-UX” à la page 74 pour savoir comment connecter physiquement un périphérique de sauvegarde au système. Consultez également la documentation fournie avec la bibliothèque ADIC/GRAU ou StorageTek.

Reportez-vous à la section “Installation de clients Windows” à la page 68 pour savoir comment connecter physiquement un périphérique de sauvegarde à un système Windows pris en charge. Consultez également la documentation fournie avec la bibliothèque ADIC/GRAU ou StorageTek.

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

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

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

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

   ```
   client client_name = DP_C1,
   #       hostname = AMU,"client1"
           ip_address = 19.18.17.15,
           requests = complete,
           options = (avc,dismount),
           volumes = ((ALL)),
           drives = ((ALL)),
           inserts = ((ALL)),
           ejects = ((ALL)),
           scratchpools = ((ALL))
   ```

2. Sur chaque client Data Protector doté d'un Agent de support Data Protector installé devant accéder aux robots de bibliothèque DAS ADIC/GRAU, modifiez le fichier `omnirc` (fichiers

<répertoire_Data_Protector>\omnirc sous Windows, /opt/omni/.omnirc sous HP-UX et Solaris et /usr/omni/omnirc sur AIX) et définissez les variables suivantes :

DAS_CLIENT — Un nom unique de client GRAU défini sur le serveur DAS. Par exemple, si le nom du client est “DP_C1”, la ligne correspondante dans le fichier omnirc est DAS_CLIENT=DP_C1.

DAS_SERVER — Le nom du serveur DAS.

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

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

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

   ```
   OB2_ACIEJECTTOTAL = 0
   ```

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

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

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

Configuration système requise

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

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

✓ Data Protector doit être installé et configuré. Pour connaître la procédure à suivre, reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d’installation (IS) de Data Protector” à la page 19 de ce chapitre.

✓ Le serveur DAS doit être en cours d'exécution.

Le logiciel DAS est requis pour contrôler la bibliothèque ADIC/GRAU. Chaque client DAS doit être doté d'un logiciel client DAS installé. Chaque action relative aux supports et aux périphériques lancée par Data Protector est d'abord transférée du client DAS au serveur DAS. Elle est ensuite transmise au module interne (AMU - Unité de gestion de l'AML) de la bibliothèque ADIC/GRAU qui contrôle le robot et déplace ou charge les supports. Lorsqu'une action est terminée, le serveur DAS répond au client DAS. Consultez la documentation fournie avec la bibliothèque ADIC/GRAU pour en savoir plus à ce sujet.

✓ Vous devez obtenir les informations suivantes avant d'installer l'Agent de support :

- Le nom d'hôte du serveur DAS (application exécutée sur l'hôte OS/2).
- La liste des lecteurs disponibles et de leurs noms DAS correspondants. Les noms des lecteurs obtenus doivent être utilisés dans la configuration des lecteurs ADIC/GRAU dans Data Protector.

  Si vous avez défini les clients DAS pour votre système ADIC/GRAU, vous pouvez obtenir cette liste avec les commandes `dasadmin` suivantes :

  ```
  dasadmin listd2 <client>
  ```

  ```
  dasadmin listd <client>
  ```

où *<client>* représente le client DAS pour lequel les lecteurs réservés doivent être affichés.

Vous pouvez appeler la commande `dasadmin` depuis le répertoire `C:\DAS\BIN` sur l'hôte OS/2 ou, dans le cas d'une installation sur d'autres systèmes, depuis le répertoire dans lequel le logiciel client DAS a été installé. Sur un système client UNIX, ce répertoire est généralement le répertoire système `/usr/local/aci/bin`.

- La liste des zones d'insertion/éjection disponibles avec les spécifications de format correspondantes.

  Vous pouvez obtenir la liste de ces zones dans la configuration graphique de l'AMS (Logiciel de gestion de l'AML) d'un hôte OS/2 :

  1. Lancez cette configuration à partir du menu `Admin -> Configuration`.
  2. Ouvrez la fenêtre `Configuration-EIF` en cliquant deux fois sur l'icône de l'unité d'E/S, puis cliquez sur le champ `Plages logiques`.
     Les zones d'insertion/éjection disponibles sont énumérées dans la zone de texte.

REMARQUE

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

- Une liste de fichiers de périphérique UNIX pour les lecteurs, si vous souhaitez installer l'Agent de support sur un système UNIX.

  Exécutez la commande système `ioscan -fn` sur votre système pour afficher les informations requises.

  Pour obtenir plus d'informations sur les fichiers de périphérique UNIX, reportez-vous à la section “Connexion d'un périphérique de sauvegarde aux systèmes HP-UX” à la page 78.

- Une liste d'adresses SCSI pour les lecteurs, si vous souhaitez installer l'Agent de support sur un système Windows. Par exemple, `scsi4:0:1:0`.

Pour obtenir plus d'informations sur les adresses SCSI, reportez-vous à la section “Connexion d'un périphérique de sauvegarde aux systèmes Windows” à la page 72.

Installation

La procédure d'installation est la suivante :

1. Distribuez le composant Agent de support aux clients à l'aide de l'interface graphique utilisateur de Data Protector et du Serveur d'installation. Pour connaître la procédure à suivre, reportez-vous à la section “Installation distante de clients Data Protector” à la page 54 de ce chapitre.
2. Installez la bibliothèque ADIC/GRAU :
   - Avec un système Windows, procédez comme suit :
     a. Copiez les bibliothèques `aci.dll`, `winrpc32.dll` et `ezrpc32.dll` dans le répertoire *<répertoire_Data_Protector>*`\bin`. (ces trois bibliothèques font partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU ; elles se trouvent sur le support d'installation ou dans le répertoire `C:\DAS\AMU\` de l'AMU-PC).
     b. Copiez également ces trois fichiers dans le répertoire *<%SystemRoot%>*`\system32`.
     c. Copiez `Portinst` et le `service Portmapper` dans le client DAS (ces éléments font partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU ; vous les trouverez sur le support d'installation).
     d. Dans le Panneau de configuration, ouvrez `Outils d'administration, Services` et lancez `portinst` pour installer `portmapper`. Vous devez relancer le client DAS pour exécuter le service `portmapper`.
     e. Après avoir réamorcé le système, vérifiez que `portmapper` et les deux `services rpc` sont exécutés (dans le Panneau de configuration, ouvrez `Outils d'administration, Services` et vérifiez l'état des services).
   - Sur un système HP-UX, copiez la bibliothèque partagée `libaci.sl` dans le répertoire `/opt/omni/lib`. Vous devez disposer des autorisations nécessaires pour accéder à ce répertoire. Vérifiez que la bibliothèque partagée dispose bien des

autorisations de lecture et d'exécution pour tout le monde (root, groupe et autre). La bibliothèque partagée `libaci.sl` fait partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU ; vous la trouverez sur le support d'installation.

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

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

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

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

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

Etape suivante

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

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

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

✓ La bibliothèque StorageTek doit être configurée et en cours d'exécution. Consultez la documentation fournie avec cette bibliothèque.

✓ Data Protector doit être installé et configuré. Reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d’installation (IS) de Data Protector” à la page 19.

✓ Vous devez obtenir les informations suivantes avant de commencer à installer un logiciel Agent de support :

- Le *<nom de l'hôte>* sur lequel ACSLS est en cours d'exécution.
- Une liste d'ID de lecteurs ACS que vous souhaitez utiliser avec Data Protector. Les ID des lecteurs obtenus doivent être utilisés dans la configuration des lecteurs StorageTek dans Data Protector. Pour afficher cette liste, connectez-vous à l'hôte où ACSLS est en cours d'exécution, puis exécutez la commande suivante :

  ```
  rlogin “ACSLS hostname” -l acssa
  ```

  Vous devrez entrer le type du terminal et attendre l'invite de commande. A l'invite ACSSA, entrez la commande suivante :

  ```
  ACSSA> query drive all
  ```

  La spécification de format d'un lecteur ACS doit être la suivante :

  ```
  ACS DRIVE: ID:#,#,#,# - (ACS num, LSM num, PANEL, DRIVE)
  ```

- Une liste d'ID DE CAP ACS disponibles avec leur spécification de format. Pour afficher cette liste, connectez-vous à l'hôte où ACSLS est en cours d'exécution, puis exécutez la commande suivante :

  ```
  rlogin “ACSLS hostname” -l acssa
  ```

  Vous devrez entrer le type du terminal et attendre l'invite de commande. A l'invite ACSSA, entrez la commande suivante :

  ```
  ACSSA> query cap all
  ```

  La spécification de format de CAP ACS doit être la suivante :

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

- Une liste de fichiers de périphérique UNIX pour les lecteurs, si vous souhaitez installer l'Agent de support sur un système UNIX.

  Exécutez la commande système `ioscan -fn` sur votre système pour afficher les informations requises.

Pour obtenir plus d'informations sur les fichiers de périphérique UNIX, reportez-vous à la section “Connexion d'un périphérique de sauvegarde aux systèmes HP-UX” à la page 78.

- Une liste d'adresses SCSI pour les lecteurs, si vous souhaitez installer l'Agent de support sur un système Windows. Par exemple, `scsi4:0:1:0`.

  Pour obtenir plus d'informations sur les adresses SCSI, reportez-vous à la section “Connexion d'un périphérique de sauvegarde aux systèmes Windows” à la page 72.

✓ Vérifiez que les lecteurs qui vont être utilisés pour Data Protector sont bien à l'état `en ligne`. Si un lecteur n'est pas `en ligne`, changez l'état à l'aide de la commande suivante sur l'hôte ACSLS :

```
vary drive <id_lecteur> online
```

✓ Vérifiez que les CAP qui seront utilisés pour Data Protector sont à l'état `en ligne` et en mode de fonctionnement `manuel`.

Si un CAP n'est pas `en ligne`, changez l'état à l'aide de la commande suivante :

```
vary cap <id_cap> online
```

Si un CAP n'est pas en mode de fonctionnement `manuel`, changez le mode à l'aide de la commande suivante :

```
set cap manual <id_cap>
```

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

La procédure d'installation est la suivante :

1. Distribuez le composant Agent de support aux clients à l'aide de l'interface graphique utilisateur de Data Protector et du Serveur d’installation pour UNIX. Pour connaître la procédure à suivre, reportez-vous à la section “Installation distante de clients Data Protector” à la page 54 de ce chapitre.
2. Exécutez le démon ACS `ssi` pour chaque client ACS :
   - Sur des clients HP-UX et Solaris, exécutez la commande suivante :

     ```
     /opt/omni/acs/ssi.sh start <nom_hôte_LS_ACS>
     ```

- Sur des clients ACS Windows, installez le service `LibAttach`. Pour plus de détails à ce sujet, reportez-vous à la documentation ACS. Vérifiez que le nom d'hôte d'ACSLS approprié est entré pendant la configuration du service `LibAttach`. Au terme d'une configuration réussie, les services `LibAttach` sont lancés automatiquement. Ils seront également lancés automatiquement après chaque réamorçage.
- Sur des clients ACS AIX, exécutez la commande suivante :

  `/usr/omni/acs/ssi.sh start <nom_hôte_LS_ACS>`

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

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

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

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

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

Installation locale de clients Novell NetWare

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

Vous pouvez installer l'Agent de disque et l'Agent général de supports Data Protector sur les systèmes exécutant Novell NetWare. Pour obtenir des informations sur les composants Data Protector, reportez-vous à la section “Composants Data Protector” à la page 63.

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

Configuration système requise

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

✓ Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

✓ Le protocole de transport TCP/IP doit être installé et en état de fonctionnement.

✓ Assurez-vous que l'un des services suivants est en cours d'exécution sur le système Windows :

- Service passerelle pour Novell NetWare.

  Ce service doit s'exécuter sur Windows lorsqu'une installation est exécutée à partir du serveur Windows.

- Client Novell pour Windows ou service client Microsoft pour NetWare.

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

✓ Connectez-vous au serveur NetWare cible (ou à l'arborescence NDS/eDirectory appropriée) à partir du système Windows.

✓ Vérifiez que vous disposez bien des droits de superviseur pour le volume SYS: sur le serveur NetWare cible.

✓ Assurez-vous qu'au moins un nom de périphérique local est libre sur le système Windows.

Clients compatibles cluster

D'autres conditions sont requises pour l'installation de clients compatibles cluster. Pour plus de détails, reportez-vous à la section “Installation d'un client” à la page 191.

Installation

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

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

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

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

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

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

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

REMARQUE

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

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

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

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

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

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

3. Avant de continuer, assurez-vous que les modules suivants sont chargés sur votre système :

   — `NETDB.NLM`

   — `TSAFS.NLM`

   — `TSANDS.NLM`

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

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

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

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

   LOAD HPINET.NLM
   ```

REMARQUE

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

```
LOAD HPINET.NLM -port <numéro_port>
```

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

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

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

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

   ```
   LOAD HPLOGIN.NLM
   ```

3. Fournissez les informations utilisateur suivantes au fichier HPLOGIN.NLM pour réussir la connexion à la base de données NDS/eDirectory :

   - Contexte NDS/eDirectory :

     Ce contexte décrit le conteneur où résident les objets utilisateur. La syntaxe du nom de ce conteneur doit être une syntaxe de nom unique. Par exemple :

     ```
     OU=SDM.O=HSL
     ```

   - Nom d'objet NDS/eDirectory :

     Il s'agit du nom commun de l'objet utilisateur qui sera utilisé comme utilisateur NDS/eDirectory valide pour la connexion à la base de données NDS/eDirectory lorsque l'Agent de disque Data Protector effectue une sauvegarde ou une restauration des NDS/eDirectory. L'utilisateur sélectionné doit se trouver dans le contexte appliqué précédemment. Par exemple :

     ```
     CN=MarcJ
     ```

si le nom unique de l'utilisateur sélectionné a pour syntaxe `.CN=MarcJ.OU=SDM.O=HSL`.

- Mot de passe d'objet NDS/eDirectory :

  Il s'agit d'un mot de passe utilisateur valide utilisé avec le nom d'utilisateur pour la connexion à la base de données NDS/eDirectory lorsqu'une sauvegarde ou une restauration de cette dernière est lancée.

  Les informations utilisateur saisies dans le module `HPLOGIN` sont encodées et stockées dans le répertoire `SYS:SYSTEM`. Il est également utilisé en association avec les modules Novell NetWare SMS qui doivent être chargés et qui doivent fonctionner.

REMARQUE

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

Si certaines modifications sont apportées à l'objet NDS/eDirectory utilisé (déplacement vers un autre conteneur, suppression, attribution d'un nouveau nom, changement de mot de passe), les informations encodées dans le répertoire `SYS:SYSTEM` doivent être mises à jour dans le module `HPLOGIN`.

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

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

REMARQUE

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

CONSEIL

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

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

Configuration de l'Agent de support

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

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

Le pilote peut être chargé automatiquement lorsque vous redémarrez le serveur si vous ajoutez une commande LOAD au fichier STARTUP.NCF. La commande doit préciser la situation du pilote, toutes les options disponibles et le numéro d'emplacement. Reportez-vous au document *Adaptec Driver User's Guide* pour obtenir la liste des options disponibles et déterminer les numéros d'emplacement.

Exemple

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

```
SET RESERVED BUFFERS BELOW 16 MEG=200

LOAD AHA2940.HAM SLOT=4 lun_enable=03
```

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

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

REMARQUE

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

CONSEIL

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

```
SCAN FOR NEW DEVICES

SCAN ALL LUNS
```

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

Etape suivante

Une fois que le logiciel Agent général de supports Data Protector est installé correctement sur la plate-forme Novell NetWare, il est conseillé de vérifier son installation. Reportez-vous à la section “Vérification de l'installation de l'Agent général de supports sous Novell NetWare” à la page B-78.

Après avoir vérifié l'installation, vous pouvez importer le client Novell NetWare dans la cellule Data Protector à l'aide de l'interface graphique utilisateur de Data Protector. Reportez-vous à l'index de l'aide en ligne (rubrique "Novell NetWare") pour plus d'informations sur les autres tâches de configuration.

Installation locale de clients OpenVMS

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

Vous pouvez installer l'Agent de disque, l'Agent général de supports et l'Interface utilisateur (interface de ligne de commande uniquement) de Data Protector sur des systèmes OpenVMS 7.3-1/IA64 8.2. Vous pouvez également installer le composant Intégration Oracle sur des systèmes utilisant OpenVMS version 7.3-1 ou supérieure. Pour obtenir des informations sur les composants Data Protector, reportez-vous à la section “Composants Data Protector” à la page 63.

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

Configuration système requise

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

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

Installation

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

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

1. Si vous disposez déjà d'un fichier d'installation PCSI, passez à l'étape 2. Pour obtenir le fichier d'installation PCSI, montez le CD d'installation et exécutez le programme `DPVMSKIT.EXE` qui se trouve dans le répertoire OpenVMS du CD. Le fichier d'installation PCSI est alors extrait dans votre répertoire par défaut ou dans celui spécifié.
2. Exécutez la commande suivante :

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

   où *`unité`*`:[`*`répertoire`*`]` est l'emplacement du fichier d'installation .PCSI.
3. Vérifiez la version du kit en répondant `YES` à l'invite :

   ```
   The following product has been selected:
   HP AXPVMS DP A06.00-xx Layered Product
   Do you want to continue? [YES]
   ```
4. Sélectionnez les composants logiciels à installer. Si vous choisissez l'installation par défaut, l'Agent de disque, l'Agent général de supports et l'Interface utilisateur seront installés. Notez que le composant Intégration Oracle (systèmes Alpha uniquement) n'est pas installé par défaut. Vous pouvez également sélectionner chaque composant séparément.

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

Exemple

```
HP AXPVMS DP A6.00-xx: HP AXPVMS Data Protector V6.00

Copyright 2006 Hewlett-Packard Development Company, L.P.

Do you want the defaults for all options? [YES] NO
Do you wish to install a disk agent for this client node?
[YES] YES
Do you wish to install a media agent for this client node?
[YES] YES
Do you wish to install the command language interface
(CLI)? [YES] YES
Do you want to review the options? [NO] YES

HP AXPVMS DP A6.00-xx: HP OpenVMS Alpha Data Protector
V6.00 [Installed]
Do you wish to install a disk agent for this client node?:
OUI
Do you wish to install a media agent for this client
node?: OUI
Do you wish to install the command language interface
(CLI)?: YES
Do you wish to install the Oracle Integration Agents? [NO]
YES

Are you satisfied with these options? [YES] YES
```

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

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

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

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

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

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

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

  Exécutez cette procédure de commande à partir des procédures `login.com` pour tous les utilisateurs qui utiliseront l'interface de ligne de commande. Plusieurs noms logiques sont définis dans cette procédure ; ils sont nécessaires pour l'exécution correcte des commandes CLI.

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

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

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

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

7. Vérifiez que vous pouvez vous connecter depuis le client OpenVMS à tous les alias TCP/IP possibles pour le Gestionnaire de cellule.
8. Importez le client OpenVMS dans la cellule Data Protector en utilisant l'interface graphique utilisateur de Data Protector comme indiqué dans la section “Importation de clients dans une cellule” à la page 197.

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

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

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

Installation dans un environnement de cluster

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

Si vous utilisez un nom d'alias TCP/IP pour le cluster, vous pouvez également définir un client pour le nom d'alias si vous utilisez un disque système commun pour le cluster. Lorsque le client alias est défini, il n'est plus nécessaire de configurer individuellement chaque nœud client. Vous avez alors le choix entre la définition du client et la définition de l'alias pour exécuter les sauvegardes et restaurations dans un cluster. Selon votre configuration, la sauvegarde ou la restauration peuvent ou non utiliser un chemin d'accès direct vers votre lecteur de bande ou votre bibliothèque de bandes.

Configuration de l'Agent de disque

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

- Les spécifications de fichier saisies dans l'interface graphique utilisateur ou transmis à l'interface de ligne de commande doivent être énoncées dans une syntaxe de type UNIX, comme par exemple :

  ```
  /disque/répertoire1/répertoire2/.../nomfichier.ext.n
  ```

  — La chaîne doit commencer par une barre de fraction, suivie du lecteur, des noms de répertoire et du nom de fichier, séparés par des barres de fraction.

  — Le nom du lecteur ne doit pas être suivi d'un deux-points.

— Utilisez un point devant le numéro de version plutôt qu'un point-virgule.

— Les spécifications de fichier pour les fichiers OpenVMS ne sont pas sensibles à la casse, excepté pour les fichiers résidant sur les disques `ODS-5`.

Exemple

Une spécification de fichier OpenVMS :

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

doit être spécifiée à Data Protector sous la forme :

```
/$1$DGA100/Users/Doe/Login.Com.1
```

REMARQUE

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

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

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

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

Configuration de l'Agent de support

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

```
$ RUN SYS$SYSTEM:SYSMAN

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

où :

`c` = K pour les bibliothèques de bandes SCSI à connexion directe.

`a` = A,B,C, …lettre de l'adaptateur pour le contrôleur SCSI.

`n` = numéro d'unité du robot de la bibliothèque de bandes.

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

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

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

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

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

Agent de support sur un cluster

Avec les périphériques reliés aux systèmes de cluster :

1. Configurez chaque lecteur et bibliothèque de bande pour qu'il puisse être accessible à partir de tous les nœuds.
2. Ajoutez le nom du nœud à la fin du nom du périphérique pour le différencier.
3. Pour les périphériques à bande, définissez un `nom de verrouillage de périphérique` dans `Devices/Properties/Settings/Advanced/Other`.

Exemple

Dans un cluster comportant les nœuds A et B, un TZ89 est connecté au nœud A et relié comme serveur au nœud B par protocole MSCP. Configurez un périphérique nommé `TZ89_A`, avec le nœud A comme client et configurez un périphérique nommé `TZ89_B`, avec le nœud B comme client. Les deux périphériques obtiennent le nom de verrouillage

de périphérique commun TZ89. Data Protector peut alors utiliser les périphériques par chacun des chemins d'accès, tout en les reconnaissant comme un périphérique unique. Si vous exécutez une sauvegarde sur le nœud B avec TZ89_A, Data Protector transfère les données du nœud B au périphérique sur le nœud A. Si vous exécutez une sauvegarde sur le nœud B avec TZ89_B, le serveur MSCP OpenVMS transfère au périphérique sur le nœud B les données du nœud A.

REMARQUE

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

Interface de ligne de commande

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

```
$ @OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COM
```

Pour une description des commandes CLI disponibles, reportez-vous à la *Référence de l'interface de ligne de commande HP OpenView Storage Data Protector*.

Intégration Oracle

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

```
-key oracle8 -desc "Oracle Integration" -nlsset 159 -nlsId
12172 -flags 0x7 -ntpath "" -uxpath "" -version A.06.00
```

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

Etape suivante

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

Installation de clients MPE/iX

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

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section "Composants Data Protector" à la page 63.

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

Configuration système requise

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

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

Installation

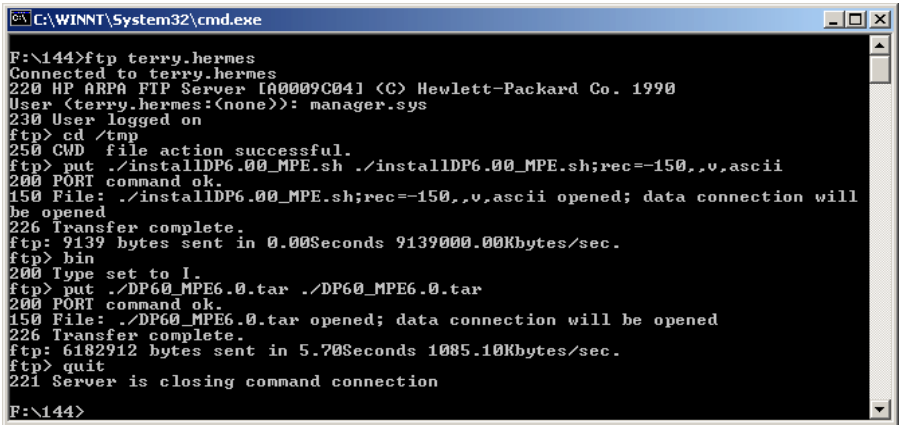
Procédez comme suit pour installer Data Protector sur le serveur MPE/iX :

1. Déplacez le script `installDP6.00_MPE.sh` et le package `DP60_MPE6.5.tar` ou `DP60_MPE7.0.tar` (selon la version du système MPE/iX) vers le répertoire `/tmp` à l'aide de l'utilitaire `ftp`. Voir l'exemple 2-1, page 128.

   Vous devez impérativement déplacer le fichier `installDP6.60_MPE.sh` avec les caractéristiques suivantes :

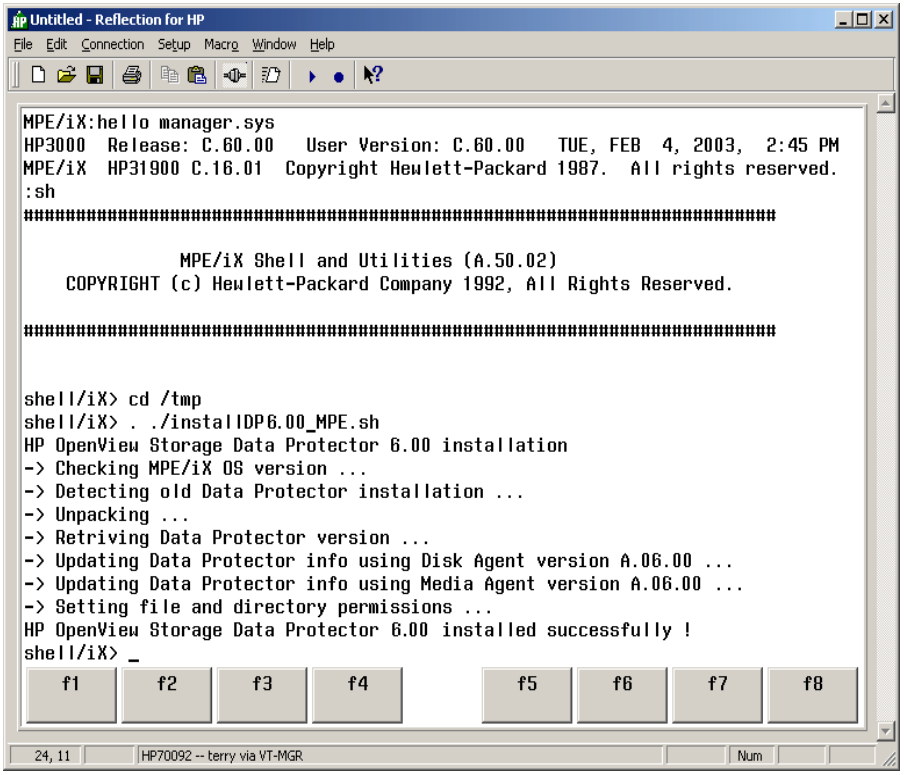
- Taille de l'enregistrement : `-150`
- Facteur de bloc : `-empty`
- Longueur variable des enregistrements du fichier : `V`
- Type des enregistrements codés : `ASCII`

Exemple 2-1 **Transfert du script installDP6.00_MPE.sh et du package DP60_MPE6.5.tar**



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

Exemple 2-2 Processus de décompactage sur le système cible



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

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

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

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

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

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

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

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

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

   `telnet <nom_hôte> 5555`

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

7. Importez le système dans la cellule Data Protector. Pour connaître la procédure à suivre, reportez-vous à la section “Importation de clients dans une cellule” à la page 197.

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

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

Installation locale de clients UNIX

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

Avant de commencer la procédure d'installation, choisissez les composants à installer sur le système client. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section “Composants Data Protector” à la page 63.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes, processeurs et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

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

Limites

Seul le shell `ksh` est pris en charge.

REMARQUE

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

Procédure

Procédez comme suit pour installer localement les clients UNIX :

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

   ```
   omnisetup.sh [-source <répertoire>] [-server <nom>]
   [-install <liste_composants>]
   ```

   où :

   - *<répertoire>* est l'emplacement où le DVD d'installation est monté. S'il n'est pas spécifié, le répertoire en cours est utilisé.
   - *<nom>* est un nom d'hôte complet du Gestionnaire de cellule de la cellule sur laquelle vous souhaitez installer le client. S'il n'est pas spécifié, le client ne sera pas automatiquement importé dans la cellule.

REMARQUE

Si vous mettez à niveau le client qui ne réside pas sur le Gestionnaire de cellule, il n'est pas nécessaire de spécifier `-install <liste_composants>`. Dans ce cas, le programme d'installation sélectionnera sans émettre d'invite les mêmes composants que ceux déjà installés sur le système.

Toutefois, pour mettre à niveau les composants du client se trouvant dans le Gestionnaire de cellule, exécutez la commande `omnisetup.sh` avec le paramètre `-install <liste_composants>` une fois la mise à niveau de Gestionnaire de cellule terminée.

- *<liste_composants>* est une liste séparée par des virgules des codes composants à installer. L'utilisation d'espaces n'est pas autorisée. Si le paramètre `-install` n'est pas spécifié, le processus d'installation vous invite à installer séparément tous les composants disponibles sur le système.

REMARQUE Dans le cas d'une mise à niveau du client, si vous ne spécifiez pas le paramètre `-install`, le processus d'installation sélectionnera, sans émettre d'invite, les composants qui étaient installés sur le système avant le début de la mise à niveau.

La liste des composants est présentée dans le tableau ci-dessous. La liste exacte des composants dépend de leur disponibilité sur ce système particulier. Les composants sont décrits au paragraphe “Composants Data Protector” à la page 63.

Tableau 2-4 Codes composants Data Protector

Code composant	Composant
`cc`	Interface utilisateur
`momgui`	Interface utilisateur MoM
`da`	Agent de disque
`ma`	Agent général de supports
`ndmp`	Agent de support NDMP
`informix`	Intégration Informix
`lotus`	Intégration Lotus
`oracle`	Intégration Oracle
`ov`	HP OpenView Network Node Manager
`sybase`	Intégration Sybase
`sap`	Intégration SAP R/3
`sapdb`	Intégration SAP DB

Tableau 2-4 Codes composants Data Protector

Code composant	Composant
db2	Intégration DB2
emc	Agent EMC Symmetrix
ssea	Agent HP StorageWorks Disk Array XP
snapa	Agent HP StorageWorks VA
smisa	Agent HP StorageWorks EVA SMIS-S
fra_ls	Support de langue français
jpn_ls	Support de langue japonais

Exemple

L'exemple ci-dessous présente l'installation des composants `Agent de disque`, `Agent général de supports`, `Interface utilisateur` et `Informix` sur un client qui sera automatiquement importé dans la cellule avec Gestionnaire de cellule `anapola` :

```
./omnisetup.sh -server anapola.company.com -install
da,ma,cc,informix
```

3. Le processus d'installation vous indique si l'installation est terminée et si le client a été importé dans la cellule Data Protector.

   Le composant `CORE` est installé la première fois qu'un composant logiciel est sélectionné pour l'installation.

   Le composant `CORE-INTEG` est installé la première fois qu'un composant du logiciel d'intégration est sélectionné pour l'installation ou la réinstallation.

Exécution de l'installation à partir du disque dur

Si vous souhaitez copier le DVD-ROM d'installation sur votre ordinateur et exécuter l'installation/la mise à niveau des clients UNIX à partir du disque dur, copiez au moins le répertoire `DP_DEPOT` et la commande `LOCAL_INSTALL/omnisetup.sh`. Par exemple, si vous copiez les packages d'installation vers `/var/dp60`, `DP_DEPOT` doit être un sous-répertoire de `/var/dp60` :

```
# pwd
/var/dp60
```

```
# ls
DP_DEPOT
omnisetup.sh
```

Après avoir copié ceci sur le disque dur, vous pouvez exécuter :

`omnisetup.sh -source` *<répertoire>* `[-server` *<nom>*`] [-install` *<liste_composants>*`]`

Notez que l'option `-source` est obligatoire. Par exemple :

```
./omnisetup.sh -source /var/dp60
```

Etape suivante

Si au cours de l'installation, vous n'avez pas spécifié le nom du Gestionnaire de cellule, le client ne sera pas importé dans la cellule. Dans ce cas, vous devez l'importer à l'aide de l'interface graphique utilisateur de Data Protector. Pour connaître la procédure à suivre, reportez-vous à la section “Importation de clients dans une cellule” à la page 197. Pour plus d'informations sur les tâches de configuration supplémentaires, reportez-vous à l'aide en ligne.

Installation des clients d'intégration Data Protector

Les intégrations Data Protector sont des composants logiciels permettant d'exécuter une sauvegarde en ligne des applications de bases de données, telles qu'Oracle ou Microsoft Exchange, avec Data Protector. Les intégrations ZDB Data Protector sont des composants logiciels permettant d'exécuter une sauvegarde ZDB à l'aide de baies de disques ZDB, telles que HP StorageWorks Enterprise Virtual Array.

Les systèmes exécutant des applications de base de données sont appelés **clients d'intégration** ; les systèmes utilisant les baies de disques ZDB pour la sauvegarde et la restauration des données sont appelés **clients d'intégration ZDB**. Ces clients sont installés à l'aide de la même procédure que tout autre client sous Windows ou UNIX, à condition que le composant logiciel approprié ait été sélectionné (par exemple, le composant `Intégration MS Exchange 2000/2003` pour la sauvegarde d'une base de données MS Exchange, le composant `Agent HP StorageWorks EVA SMI-S` pour une sauvegarde avec temps d'indisponibilité nul sur HP StorageWorks Enterprise Virtual Array, etc.).

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes, processeurs et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.
- Une licence est nécessaire pour utiliser l'intégration Data Protector avec une application de base de données (à l'exception de l'intégration VSS). Pour plus d'informations sur l'attribution des licences, consultez la section “Extensions fonctionnelles” à la page A-9.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d’installation (éventuellement pour une installation distante) doivent être installés sur votre réseau. Reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d’installation (IS) de Data Protector” à la page 19 pour de plus amples informations.

Avant de lancer la procédure d'installation, choisissez les autres composants logiciels Data Protector à installer sur le client avec un composant d'intégration. Pour consulter la liste des composants logiciels de Data Protector et leurs descriptions, reportez-vous à la section “Composants Data Protector” à la page 63.

Notez que dans les situations exposées ci-dessous, vous devez installer les composants Data Protector suivants :

- Composant `Agent de disque` pour pouvoir sauvegarder des données de système de fichiers avec Data Protector. Vous pouvez utiliser l'Agent de disque dans les cas suivants :
  - — Pour exécuter une sauvegarde du système de fichiers de données importantes pour lesquelles la sauvegarde de l'application de base de données *ne peut pas* être utilisée.
  - — Pour exécuter un essai de sauvegarde du système de fichiers d'un serveur d'application de base de données (serveur Oracle ou MS SQL Server, par exemple). Vous devez procéder à un essai de sauvegarde de système de fichier *avant* de configurer l'intégration Data Protector avec une application de base de données et résoudre les problèmes - notamment de communication - liés à l'application et à Data Protector.
  - — Pour exécuter une image disque et un client ZDB de système de fichiers.
  - — Pour effectuer une restauration à partir d'un support de données de sauvegarde vers le système d'application sur le réseau LAN dans le cas d'intégrations ZDB SAP R/3.
- Composant `Interface utilisateur` pour obtenir l'accès à l'interface graphique utilisateur et à l'interface de ligne de commande de Data Protector sur le client d'intégration de Data Protector.
- Composant `Agent général de supports` si des périphériques de sauvegarde sont connectés au client d'intégration Data Protector. Sur les clients Data Protector utilisés pour accéder à un lecteur dédié NDMP via le serveur NDMP, l'`Agent de support NDMP` est requis.

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

Pour plus d'informations sur des clients d'intégration spécifiques, reportez-vous aux paragraphes correspondants ci-après :

- Clients Microsoft Exchange Server
- Clients MS SQL
- Clients Sybase
- Clients Informix Server
- Clients SAP R/3
- Clients SAP DB
- Clients Oracle
- Clients DB2
- Clients NNM
- Clients NDMP
- Clients Cliché instantané de volumes MS
- Clients Lotus Notes/Domino Server
- Intégration EMC Symmetrix
- Intégration de HP StorageWorks XP
- Intégration de HP StorageWorks Virtual Array
- Intégration de HP StorageWorks Enterprise Virtual Array

Une fois que vous avez terminé l'installation du logiciel d'intégration Data Protector sur les clients d'intégration Data Protector comme la décrivent les sections indiquées, reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector*, au *Guide de l'administrateur HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul* ou au *Guide d'intégration HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul* pour configurer les clients d'intégration Data Protector.

Installation en local

Si vous ne disposez pas d'un Serveur d'installation pour le système d'exploitation installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation Windows ou UNIX, selon la plate-forme sur laquelle vous installez un client.

Reportez-vous à la section “Installation de clients Windows” à la page 68 ou “Installation locale de clients UNIX” à la page 130 pour connaître la procédure de cette installation.

Si vous ne choisissez pas de Gestionnaire de cellule pendant l'installation, le système du client doit être importé manuellement dans la cellule après l'installation en local. Reportez-vous également à la section “Importation de clients dans une cellule” à la page 197.

Installation à distance

Vous devez installer le logiciel client à partir du Serveur d’installation pour UNIX sur les systèmes clients utilisant l'interface graphique utilisateur de Data Protector. Pour connaître la procédure détaillée pour installer le logiciel à distance, reportez-vous à la section “Installation distante de clients Data Protector” à la page 54.

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

Installation des intégrations compatibles cluster

Les clients d'intégration Data Protector compatibles cluster doivent être installés localement, à partir du DVD-ROM, sur chaque nœud cluster. Lors de la configuration locale du client, installez les composants logiciels d'intégration appropriés (tels que `Intégration Oracle` ou `Agent HP StorageWorks EVA SMI-S`) en plus des autres composants logiciels client.

Vous pouvez également installer une application de base de données compatible cluster et un Agent ZDB sur le Gestionnaire de cellule Data Protector. Sélectionnez le composant logiciel d'intégration approprié lors de la configuration du Gestionnaire de cellule.

La procédure d'installation dépend de l'environnement de cluster dans lequel vous installez votre client d'intégration. Consultez les paragraphes relatifs à la gestion de clusters correspondant à votre système d'exploitation :

- “Installation de Data Protector sur MC/ServiceGuard” à la page 177.
- “Installation de Data Protector sur Microsoft Cluster Server” à la page 179.

- “Installation de clients Data Protector sur un cluster Veritas” à la page 190.
- “Installation de clients Data Protector sur un cluster Novell NetWare” à la page 191.

Pour plus d'informations sur la gestion de clusters, reportez-vous à l'index de l'aide en ligne (rubrique "cluster, MC/ServiceGuard") et au *Guide conceptuel HP OpenView Storage Data Protector*.

Etape suivante

Une fois l'installation terminée, reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector* approprié pour obtenir des informations sur la configuration de l'intégration.

Clients Microsoft Exchange Server

Votre serveur Microsoft Exchange est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données Microsoft Exchange Server, vous devez sélectionner le composant `Intégration MS Exchange 2000/2003` lors de la procédure d'installation.

L'agent d'intégration Boîte aux lettres unique de Microsoft Exchange sera installé en tant que partie du package d'intégration Microsoft Exchange Server de Data Protector.

Clients MS SQL

Votre serveur Microsoft SQL Server est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données Microsoft SQL Server, vous devez sélectionner le composant `Intégration MS SQL 7.0/2000` lors de la procédure d'installation.

Clients Sybase

Votre serveur Sybase Backup Server est supposé sous tension et en cours de fonctionnement.

Pour sauvegarder la base de données Sybase, vous devez sélectionner les composants Data Protector suivants lors de la procédure d'installation :

- `Intégration Sybase` - pour la sauvegarde d'une base de données Sybase.
- `Agent de disque` - installez l'Agent de disque pour deux raisons :
  - — Pour exécuter une sauvegarde du système de fichiers de Sybase Backup Server. Effectuez cette sauvegarde *avant* de configurer votre intégration Data Protector Sybase et résolvez tous les problèmes liés à Sybase Backup Server et à Data Protector.
  - — Pour exécuter une sauvegarde du système de fichiers de données importantes pour lesquelles Sybase Backup Server *ne peut pas* être utilisé.

Clients Informix Server

Votre serveur Informix Server est supposé sous tension et en cours de fonctionnement.

Pour sauvegarder la base de données Informix Server, vous devez sélectionner les composants Data Protector suivants lors de la procédure d'installation :

- `Intégration Informix` - pour la sauvegarde d'une base de données Informix Server.
- `Agent de disque` - installez l'Agent de disque pour deux raisons :
  - — Pour exécuter une sauvegarde du système de fichiers Informix Server. Effectuez cette sauvegarde *avant* de configurer votre intégration Data Protector Informix Server et résolvez tous les problèmes liés à Informix Server et à Data Protector.
  - — Pour exécuter une sauvegarde du système de fichiers pour les données Informix Server importantes (telles que le fichier ONCONFIG, le fichier `sqlhosts`, le fichier d'amorçage de secours ON-Bar, `oncfg_<INFORMIXSERVER>.<SERVERNUM>`, les fichiers de configuration, etc.) qui *ne peuvent pas* être sauvegardés avec ON-Bar.

Clients SAP R/3

Votre serveur SAP R/3 Database est supposé sous tension et en cours de fonctionnement.

REMARQUE Les spécifications de sauvegarde de l'intégration SAP R/3 Data Protector sont entièrement compatibles avec la version antérieure de Data Protector. Data Protector exécute toutes les spécifications de sauvegarde créées par les versions antérieures. En revanche, vous ne pouvez pas utiliser sur une version antérieure de Data Protector les spécifications de sauvegarde créées avec la version actuelle.

Pour pouvoir sauvegarder la base de données SAP R/3, sélectionnez les composants suivants lors de la procédure d'installation :

- `Intégration SAP R/3`
- `Intégration Oracle`

  Installez ce composant si vous avez l'intention d'utiliser Oracle Recovery Manager pour sauvegarder et restaurer les fichiers de base de données SAP R/3.

- `Agent de disque`

  Data Protector requiert l'installation d'un Agent de disque sur les serveurs de sauvegarde (clients comportant des données de système de fichiers à sauvegarder).

Clients SAP DB

Votre serveur SAP DB est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données SAP DB, vous devez sélectionner les composant Data Protector suivants lors de la procédure d'installation :

- `Intégration SAP DB` - pour pouvoir exécuter une sauvegarde en ligne intégrée d'une base de données SAP DB.
- `Agent de disque` - pour pouvoir exécuter une sauvegarde hors ligne non intégrée d'une base de données SAP DB.

Clients Oracle

Votre serveur Oracle est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données Oracle, vous devez sélectionner le composant `Intégration Oracle` lors de la procédure d'installation.

Vérification de la bibliothèque orasbt.dll

Après l'installation, vous devez démarrer les services Oracle et vérifier que la bibliothèque de base de données *<Libellé_lecteur>*:*<%SystemRoot%>*\system32\orasbt.dll Data Protector est chargée :

1. Dans l'explorateur Windows, accédez au répertoire *<Libellé_lecteur>*:*<%SystemRoot%>*\system32 et cliquez avec le bouton droit de la souris sur `orasbt.dll`.
2. Sélectionnez `Propriétés` et cliquez sur l'onglet `Version` de la fenêtre `Propriétés de orasbt.dll`. Dans le champ `Description` doit figurer le fichier décrit comme une partie de l'intégration Data Protector.

Pour vérifier que `orasbt.dll` est chargé correctement, copiez le fichier et essayez de supprimer l'original. Un message indiquant que le fichier est en cours d'utilisation doit apparaître.

Figure 2-20 **Message d'erreur**

OpenVMS

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

```
-key oracle8 -desc "Oracle Integration" -nlsset 159 -nlsId
12172 -flags 0x7 -ntpath "" -uxpath "" -version A.06.00
```

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

Clients DB2

Votre serveur DB2 est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données DB2, vous devez sélectionner les composants `Intégration DB2` et `Agent de disque` lors de la procédure d'installation.

Dans un environnement à partition physique, installez les composants `Intégration DB2` et `Agent de disque` sur chaque nœud physique (système) sur lequel réside la base de données.

REMARQUE Connectez-vous comme utilisateur `root` pour effectuer l'installation.

Clients NNM

Votre système NNM est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données NNM, vous devez sélectionner les composants `Intégration de sauvegarde NNM HP OpenView` et `Agent de disque` lors de la procédure d'installation. Vous aurez besoin de l'Agent de disque pour exécuter les scripts antérieurs et postérieurs à la sauvegarde utilisés pour les opérations de sauvegarde.

Clients NDMP

Votre serveur NDMP est supposé sous tension et en cours de fonctionnement.

Au cours de la procédure d'installation, sélectionnez l'`agent de support NDMP` et installez-le sur tous les clients Data Protector ayant accès aux lecteurs NDMP dédiés.

REMARQUE Dans le cas où un client Data Protector ne doit pas être utilisé pour accéder à un lecteur NDMP dédié par le serveur NDMP et sera uniquement utilisé pour commander le robot de la bibliothèque, on peut installer sur ce client soit l'`Agent de support NDMP`, soit l'`Agent général de supports`.

Notez que seul un Agent de support peut être installé sur un client Data Protector.

Clients Cliché instantané de volumes MS

Condition préalable

Le composant Intégration MS Volume Shadow Copy est pris en charge par le système d'exploitation Windows Server 2003.

Pour pouvoir effectuer des clichés instantanés de volume des modules d'écriture compatibles VSS, vous devez sélectionner le composant `Intégration MS Volume Shadow Copy` lors de la procédure d'installation.

Si vous souhaitez effectuer des sauvegardes transportables VSS, Windows Advanced Server 2003 est nécessaire. Installez les composants suivants sur les systèmes de sauvegarde et d'application : `Intégration MS Volume Shadow Copy` et `Agent général de supports`.

Clients Lotus Notes/Domino Server

Votre serveur Lotus Notes/Domino Server est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données Lotus Notes/Domino Server, vous devez sélectionner les composants `Intégration Lotus` et `Agent de disque` lors de la procédure d'installation. Vous avez besoin du composant `Agent de disque` pour pouvoir sauvegarder les données du système de fichiers avec Data Protector pour les tâches suivantes :

- Sauvegarde des données importantes qui *ne peuvent* être sauvegardées avec l'agent d'intégration Lotus. Il s'agit de fichiers "non-bases de données", qui doivent être sauvegardés pour fournir une solution complète de protection des données pour un serveur Lotus Domino R5, par exemple `notes.ini`, `desktop.dsk` et tous les fichiers `*.id`.

- Essai de sauvegarde du système de fichiers pour résoudre les problèmes - notamment de communication - liés à l'application et à Data Protector.

Intégration EMC Symmetrix

Pour intégrer EMC Symmetrix à Data Protector, installez les composants logiciels Data Protector suivants sur les systèmes d'application et de sauvegarde :

- `Agent EMC Symmetrix` (SYMA)
- `Agent général de supports`

  Installez le composant `Agent général de supports` sur le système de sauvegarde pour sauvegarder les données en bloc. Installez-le sur le système d'application pour sauvegarder les journaux d'archive ou pour restaurer le système.

- `Agent de disque`

  Installez le composant `Agent de disque` sur les systèmes d'application et de sauvegarde pour exécuter des sauvegardes ZDB d'image disque et de système de fichiers. Les clients sans Agent de disque ne sont pas répertoriés dans les listes déroulantes `Système d'application` et `Système de sauvegarde` lors de la création d'une spécification ZDB.

Installation sur un cluster

Vous pouvez installer l'intégration EMC Symmetrix dans un environnement de cluster. Pour connaître les configurations de clusters prises en charge et la configuration requise pour l'installation, reportez-vous au *Guide de l'administrateur HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

Intégration à d'autres applications

Si vous souhaitez installer l'intégration EMC Symmetrix avec une application de base de données, installez le composant Data Protector spécifique à l'intégration de cette application sur les systèmes d'application et de sauvegarde, et effectuez les tâches spécifiques à cette intégration. Vous pouvez installer l'intégration EMC Symmetrix avec Oracle et SAP R/3.

Intégration EMC Symmetrix avec Oracle

Configuration système requise

- Les logiciels suivants doivent être installés et configurés sur des disques non mis en miroir du système d'application :

  ✓ Oracle Enterprise Server (RDBMS)

  ✓ Logiciel Oracle Net8

  ✓ SQL*Plus

  Il est nécessaire d'installer au moins Oracle Server et SQL*NET V2 ou NET8.

- Les fichiers de la base de données Oracle utilisés par le système d'application doivent être installés sur des périphériques EMC Symmetrix qui sont mis en miroir sur le système de sauvegarde.

  La base de données peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers. Les fichiers Oracle suivants doivent être mis en miroir :

  ✓ Fichiers de données

  ✓ Fichier de contrôle

  ✓ Fichiers journaux de rétablissement en ligne

  Les fichiers journaux de rétablissement archivés doivent résider sur des disques qui ne sont pas en miroir.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez la base de données du catalogue de récupération Oracle.

   Reportez-vous à la documentation Oracle pour obtenir des informations sur l'installation de la base de données du catalogue de récupération Oracle sur le système d'application, sur des disques n'étant pas en miroir. Laissez le catalogue de récupération non enregistré.

2. Installez les composants logiciels Data Protector suivants :

   - `Agent EMC Symmetrix` - sur le système d'application et le système de sauvegarde.

- `Intégration Oracle` - si vous souhaitez utiliser la méthode de jeu de sauvegardes ZDB, installez ce composant à la fois sur le système d'application et sur le système de sauvegarde ; si vous souhaitez utiliser la méthode proxy-copy ZDB, installez-le sur le système d'application seulement.

Intégration EMC Symmetrix avec SAP R/3

Configuration système requise

- Les logiciels Oracle suivants doivent être installés sur le système d'application :
  - ✓ Oracle Enterprise Server (RDBMS)
  - ✓ Logiciel Oracle Net8
  - ✓ SQL*Plus
- La base de données du système d'application peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers. Les fichiers de données Oracle *doivent* résider sur des volumes source en baie de disques.

  Pour la sauvegarde hors ligne, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* aussi résider sur une baie de disques.

  Les fichiers journaux de rétablissement archivés ne doivent pas nécessairement résider sur une baie de disques.
- L'utilisateur `ora<ORACLE_SID>` doit être créé sur le système d'application dans le groupe principal `dba`.

  L'utilisateur UNIX `<ORACLE_SID>adm` doit être créé sur le système d'application dans le groupe UNIX `sapsys`.
- Le logiciel SAP R/3 doit être correctement installé sur le système d'application.

  Les répertoires standard suivants doivent être installés sur le système d'application après l'installation de SAP R/3 :

REMARQUE

L'emplacement des répertoires dépend des variables d'environnement. Reportez-vous à la documentation SAP R/3 pour plus d'informations.

`<ORACLE_HOME>/dbs` - les profils Oracle et SAP R/3

<ORACLE_HOME>/bin - les fichiers binaires Oracle

<SAPDATA_HOME>/sapbackup - le répertoire SAPBACKUP contenant les fichiers journaux BRBACKUP

<SAPDATA_HOME>/sapbackup - le répertoire SAPARCH contenant les fichiers journaux BRARCHIVE

<SAPDATA_HOME>/sapreorg

<SAPDATA_HOME>/sapcheck

<SAPDATA_HOME>/saptrace

/usr/sap/*<ORACLE_SID>*/SYS/exe/run

Si les six derniers répertoires ne sont pas aux emplacements indiqués ci-dessus, créez les liens appropriés vers eux.

Le propriétaire du répertoire /usr/sap/*<ORACLE_SID>*/SYS/exe/run doit être l'utilisateur UNIX ora*<ORACLE_SID>*. Le propriétaire des fichiers SAP R/3 doit être l'utilisateur UNIX ora*<ORACLE_SID>* et le groupe UNIX dba avec le bit setuid à 1 (chmod 4755 ...). L'exception est le fichier BRRESTORE, dont le propriétaire doit être l'utilisateur UNIX *<ORACLE_SID>*adm.

Exemple

Si *<ORACLE_SID>* est PROD, les droits à l'intérieur du répertoire /usr/sap/*<ORACLE_SID>*/SYS/exe/run doivent ressembler à ce qui suit :

```
-rwsr-xr-x   1 oraprod dba 4598276 Apr 17  1998 brarchive
-rwsr-xr-x   1 oraprod dba 4750020 Apr 17  1998 brbackup
-rwsr-xr-x   1 oraprod dba 4286707 Apr 17  1998 brconnect
-rwsr-xr-x   1 prodadm sapsys 430467 Apr 17  1998 brrestore
-rwsr-xr-x   1 oraprod dba 188629 Apr 17  1998 brtools
-rwsr-xr-x   1 oraprod dba 6081400 May  8  1998 sapdba.
```

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez SAP R/3 BRTOOLS sur le système d'application.
2. Installez les composants logiciels Data Protector suivants :
   - Agent EMC Symmetrix - sur le système d'application et le système de sauvegarde
   - Intégration SAP R/3 - sur le système d'application uniquement
   - Agent de disque - sur le système d'application et le système de sauvegarde

Intégration de HP StorageWorks XP

Pour intégrer HP StorageWorks XP à Data Protector, installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :

- `Agent HP StorageWorks XP`
- `Agent général de supports`

  Installez le composant `Agent général de supports` sur le système de sauvegarde pour sauvegarder les données en bloc. Installez-le sur le système d'application pour sauvegarder les journaux d'archive ou pour restaurer le système.

- `Agent de disque`

  Installez le composant `Agent de disque` sur les systèmes d'application et de sauvegarde pour exécuter des sauvegardes ZDB d'image disque et de système de fichiers. Les clients sans Agent de disque ne sont pas répertoriés dans les listes déroulantes `Système d'application` et `Système de sauvegarde` lors de la création d'une spécification ZDB.

Installation sur un cluster

Vous pouvez installer l'intégration HP StorageWorks XP dans un environnement de cluster. Pour connaître les configurations de clusters prises en charge et la configuration requise pour l'installation, reportez-vous au *Guide de l'administrateur HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

Intégration à d'autres applications

Si vous souhaitez installer l'intégration HP StorageWorks XP avec une application de base de données, installez le composant Data Protector spécifique à l'intégration de cette application sur les systèmes d'application et de sauvegarde, et effectuez les tâches spécifiques à cette intégration. Vous pouvez installer l'intégration HP StorageWorks XP avec Oracle, SAP R/3, Microsoft Exchange Server et Microsoft SQL Server.

Intégration HP StorageWorks XP avec Oracle

Configuration système requise

- Les logiciels suivants doivent être installés et configurés sur les volumes source du système d'application :

  ✓ Oracle Enterprise Server (RDBMS)

✓ Logiciel Oracle Net8

✓ SQL*Plus

Il est nécessaire d'installer au moins Oracle Server et SQL*NET V2 ou NET8.

- Les fichiers de la base de données Oracle sur le système d'application doivent être installés sur des périphériques logiques HP StorageWorks Disk Array XP qui sont mis en miroir sur le système de sauvegarde.

  Selon l'emplacement du fichier de contrôle Oracle, des fichiers journaux de rétablissement en ligne et du fichier SPFILE Oracle9i/10g, les deux options suivantes sont possibles :

  — Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE Oracle9i/10g résident sur un groupe de volumes (si LVM est utilisé) ou un volume source **différent** des fichiers de données Oracle.

  La restauration instantanée est activée par défaut dans ce type de configuration.

  — Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE Oracle9i/10g résident sur le **même** groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle.

  Par défaut, la restauration instantanée *n'est pas* activée dans ce type de configuration. Vous pouvez l'activer en définissant les variables `omnirc` `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Pour plus d'informations, reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

  Les fichiers journaux de rétablissement archivés Oracle ne doivent pas nécessairement résider sur des volumes source.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez la base de données du catalogue de récupération Oracle.

Reportez-vous à la documentation Oracle pour obtenir des informations sur l'installation de la base de données du catalogue de récupération Oracle sur le système d'application, sur des disques n'étant pas en miroir. Laissez le catalogue de récupération non enregistré.

2. Installez les composants logiciels Data Protector suivants :

   - `Agent HP StorageWorks XP` - sur le système d'application et le système de sauvegarde.
   - `Intégration Oracle` - si vous souhaitez utiliser la méthode de jeu de sauvegardes ZDB, installez ce composant à la fois sur le système d'application et sur le système de sauvegarde ; si vous souhaitez utiliser la méthode proxy-copy ZDB, installez-le sur le système d'application seulement.

Intégration de HP StorageWorks XP avec SAP R/3

Configuration système requise

- Les logiciels Oracle suivants doivent être installés et configurés sur les volumes source de la baie de disques :

  ✓ Oracle Enterprise Server (RDBMS)

  ✓ Logiciel Oracle Net8

  ✓ SQL*Plus

  Il est nécessaire d'installer au moins Oracle Server et SQL*NET V2 ou NET8.

- La base de données du système d'application peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers. Les fichiers de données Oracle *doivent* résider sur des volumes source en baie de disques.

  Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas nécessairement résider sur une baie de disques.

  Pour la *sauvegarde hors ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* résider sur une baie de disques. Toutefois, notez les points suivants :

— Si le fichier de contrôle Oracle8i/9i, les journaux de rétablissement en ligne et le fichier SPFILE Oracle9i résident sur un groupe de volumes (si LVM est utilisé) ou un volume source **différent** des fichiers de données Oracle8i/9i, la restauration instantanée *est* activée.

— Si le fichier de contrôle Oracle8i/9i, les journaux de rétablissement en ligne et le fichier SPFILE Oracle9i résident sur le **même** groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle8i/9i, la restauration instantanée *n'est pas* activée. Vous pouvez l'activer en définissant les variables `omnirc` `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Pour plus d'informations, reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

Les fichiers journaux de rétablissement archivés ne doivent pas nécessairement résider sur une baie de disques.

- L'utilisateur `ora<ORACLE_SID>` doit être créé sur le système d'application dans le groupe principal `dba`.

  Sur les systèmes UNIX, l'utilisateur UNIX `<ORACLE_SID>adm` doit être créé sur le système d'application dans le groupe UNIX `sapsys`.

- Le logiciel SAP R/3 doit être correctement installé sur le système d'application.

  Les répertoires standard suivants doivent être installés sur le système d'application après l'installation de SAP R/3 :

REMARQUE L'emplacement des répertoires dépend des variables d'environnement (systèmes UNIX) ou de registre (systèmes Windows). Reportez-vous à la documentation SAP R/3 pour plus d'informations.

`<ORACLE_HOME>/dbs` (systèmes UNIX)
`<ORACLE_HOME>\database` (systèmes Windows - les profils Oracle et SAP R/3)

`<ORACLE_HOME>/bin ou` (systèmes UNIX)
`<ORACLE_HOME>\bin` (systèmes Windows) - les fichiers binaires Oracle

<SAPDATA_HOME>/sapbackup (systèmes UNIX)
<SAPDATA_HOME>\sapbackup (systèmes Windows) - le répertoire SAPBACKUP avec fichiers journaux BRBACKUP

<SAPDATA_HOME>/sapbarch (systèmes UNIX)
<SAPDATA_HOME>\sapbarch (systèmes Windows) - le répertoire SAPARCH avec fichiers journaux BRARCHIVE

<SAPDATA_HOME>/sapreorg (systèmes UNIX)
<SAPDATA_HOME>\sapreorg (systèmes Windows)

<SAPDATA_HOME>/sapcheck (systèmes UNIX)
<SAPDATA_HOME>\sapcheck (systèmes Windows)

<SAPDATA_HOME>/saptrace (systèmes UNIX)
<SAPDATA_HOME>\saptrace (systèmes Windows)

/usr/sap/*<ORACLE_SID>*/SYS/exe/run (systèmes UNIX)
BRTOOLS (systèmes Windows)

Systèmes UNIX

Sur les systèmes UNIX, si les six derniers répertoires ne sont pas aux emplacements indiqués ci-dessus, créez les liens appropriés vers eux.

Sur les systèmes UNIX, le propriétaire du répertoire /usr/sap/*<ORACLE_SID>*/SYS/exe/run doit être l'utilisateur UNIX ora*<ORACLE_SID>*. Le propriétaire des fichiers SAP R/3 doit être l'utilisateur UNIX ora*<ORACLE_SID>* et le groupe UNIX dba avec le bit setuid à 1 (chmod 4755 ...). L'exception est le fichier BRRESTORE, dont le propriétaire doit être l'utilisateur UNIX *<ORACLE_SID>*adm.

Exemple UNIX

Si *<ORACLE_SID>* est PROD, les droits à l'intérieur du répertoire /usr/sap/*<ORACLE_SID>*/SYS/exe/run doivent ressembler à ce qui suit :

```
-rwsr-xr-x   1 oraprod dba 4598276 Apr 17  1998 brarchive
-rwsr-xr-x   1 oraprod dba 4750020 Apr 17  1998 brbackup
-rwsr-xr-x   1 oraprod dba 4286707 Apr 17  1998 brconnect
-rwsr-xr-x   1 prodadm sapsys 430467 Apr 17  1998
brrestore
-rwsr-xr-x   1 oraprod dba 188629 Apr 17  1998 brtools
-rwsr-xr-x   1 oraprod dba 6081400 May  8  1998 sapdba.
```

Systèmes Windows

Sur les systèmes Windows, le partage SAPMNT doit être créé sur le système d'application et doit contenir le sous-répertoire *<SAPDATA_HOME>*.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez SAP R/3 BRTOOLS sur le système d'application.
2. Installez les logiciels d'intégration Data Protector.

   Sur les systèmes Windows, les composants logiciels de Data Protector doivent être installés avec le compte administrateur SAP R/3, et ce groupe doit être inclus dans le groupe local `ORA_DBA` ou `ORA_<SID>_DBA` sur le système où l'instance SAP R/3 est exécutée.

   Installez les composants logiciels Data Protector suivants :

   - `Agent HP StorageWorks XP` - sur le système d'application et le système de sauvegarde
   - `Intégration SAP R/3` - sur le système d'application uniquement
   - `Agent de disque` - sur le système d'application et le système de sauvegarde

Intégration HP StorageWorks XP avec Microsoft Exchange Server

Condition préalable

La base de données Microsoft Exchange Server doit être installée sur le système d'application, sur les volumes (périphériques logiques) HP StorageWorks Disk Array XP qui sont mis en miroir sur le système de sauvegarde. La mise en miroir peut concerner BC ou CA et la base de données installée sur un système de fichiers. Les objets suivants doivent être présents sur les volumes en miroir :

- Banque d'informations Microsoft (MIS)
- Service gestionnaire de clés (KMS, facultatif)
- Service de réplication de sites (SRS, facultatif)

Pour pouvoir sauvegarder des journaux de transactions, désactivez l'enregistrement circulaire sur le serveur Microsoft Exchange.

Procédure d'installation

Installez les composants logiciels Data Protector suivants :

- `Agent HP StorageWorks XP` - sur le système d'application et le système de sauvegarde
- `Intégration MS Exchange 2000/2003` - sur le système d'application uniquement

Intégration HP StorageWorks XP avec Microsoft SQL Server

Condition préalable

Microsoft SQL Server doit être installé sur le système d'application. Les bases de données utilisateur *doivent* se trouver sur les volumes source en baie de disques, tandis que les bases de données système peuvent être installées n'importe où. Cependant, si les bases de données système sont elles aussi installées sur la baie de disques, elles *doivent* l'être sur des volumes sources *différents* de ceux des bases de données utilisateur.

Procédure d'installation

Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :

- `Agent HP StorageWorks XP`
- `Intégration MS SQL 7.0/2000`

Intégration de HP StorageWorks Virtual Array

Pour intégrer HP StorageWorks VA à Data Protector, installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :

- `Agent HP StorageWorks VA`
- `Agent général de supports`

  Installez le composant `Agent général de supports` sur le système de sauvegarde pour sauvegarder les données en bloc. Installez-le sur le système d'application pour sauvegarder les journaux d'archive ou pour restaurer le système.

- `Agent de disque`

  Installez le composant `Agent de disque` sur les systèmes d'application et de sauvegarde pour exécuter des sauvegardes ZDB d'image disque et de système de fichiers. Les clients sans Agent de disque ne sont pas répertoriés dans les listes déroulantes `Système d'application` et `Système de sauvegarde` lors de la création d'une spécification ZDB.

Installation sur un cluster

Vous pouvez installer l'intégration HP StorageWorks VA dans un environnement de cluster. Pour connaître les configurations de clusters prises en charge et la configuration requise pour l'installation, reportez-vous au *Guide de l'administrateur HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

Intégration à d'autres applications

Si vous souhaitez installer l'intégration HP StorageWorks VA avec une application de base de données, installez le composant Data Protector spécifique à l'intégration de cette application sur les systèmes d'application et de sauvegarde, et effectuez les tâches spécifiques à cette intégration. Vous pouvez installer l'intégration HP StorageWorks VA avec Oracle, SAP R/3, Microsoft Exchange Server et Microsoft SQL Server.

Intégration HP StorageWorks VA avec Oracle

Configuration système requise

- Les logiciels suivants doivent être installés et configurés sur les volumes source du système d'application et sur le système de sauvegarde pour la méthode de jeu de sauvegardes ZDB :

  ✓ Oracle Enterprise Server (RDBMS)

  ✓ Logiciel Oracle Net8/9

  ✓ SQL*Plus

  Le logiciel Oracle installé sur le système de sauvegarde doit l'être dans le même répertoire que sur le système d'application. Les binaires doivent être identiques à ceux du système d'application. Vous pouvez y parvenir en copiant les fichiers et l'environnement système du système d'application vers le système de sauvegarde ou par une installation "propre" des binaires Oracle sur le système de sauvegarde avec les mêmes paramètres d'installation que sur le système d'application.

  Il est nécessaire d'installer au moins Oracle Server et SQL*NET V2 ou NET8/9.

- Les fichiers de base de données Oracle utilisés par le système d'application doivent être installés sur les volumes source qui seront dupliquées à l'aide de l'Agent VA (SNAPA).

  Selon l'emplacement du fichier de contrôle Oracle, des fichiers journaux de rétablissement en ligne et du fichier SPFILE Oracle9i/10g, les deux options suivantes sont possibles :

  — Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE Oracle9i/10g résident sur un groupe de volumes (si LVM est utilisé) ou un volume source **différent** des fichiers de données Oracle.

La restauration instantanée est activée par défaut dans ce type de configuration.

— Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE Oracle9i/10g résident sur le **même** groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle.

Par défaut, la restauration instantanée *n'est pas* activée dans ce type de configuration. Vous pouvez l'activer en définissant les variables `omnirc` `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF_OLF` et `ZDB_ORA_NO_CHECKCONF_IR`. Pour plus d'informations, reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

Les fichiers journaux de rétablissement archivés Oracle ne doivent pas nécessairement résider sur des volumes source.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez la base de données du catalogue de récupération Oracle.

   Reportez-vous à la documentation Oracle pour obtenir des informations sur l'installation de la base de données du catalogue de récupération Oracle sur le système d'application. Laissez le catalogue de récupération non enregistré.

2. Installez les composants logiciels Data Protector suivants :

   - `Agent HP StorageWorks VA` - sur le système d'application et le système de sauvegarde.
   - `Intégration Oracle` - si vous souhaitez utiliser la méthode de jeu de sauvegardes ZDB, installez ce composant à la fois sur le système d'application et sur le système de sauvegarde ; si vous souhaitez utiliser la méthode proxy-copy ZDB, installez-le sur le système d'application seulement.

Intégration de HP StorageWorks VA avec SAP R/3

Configuration système requise

- Les logiciels Oracle suivants doivent être installés sur les volumes sources du système d'application :

  ✓ Oracle Enterprise Server (RDBMS)

  ✓ Logiciel Oracle Net8

✓ SQL*Plus

Il est nécessaire d'installer au moins Oracle Server et SQL*NET V2 ou NET8.

- La base de données du système d'application peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers. Les fichiers de données Oracle *doivent* résider sur des volumes source en baie de disques.

  Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas nécessairement résider sur une baie de disques.

  Pour la *sauvegarde hors ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* résider sur une baie de disques. Toutefois, notez les points suivants :

  — Si le fichier de contrôle Oracle8i/9i, les journaux de rétablissement en ligne et le fichier SPFILE Oracle9i résident sur un groupe de volumes (si LVM est utilisé) ou un volume source **différent** des fichiers de données Oracle8i/9i, la restauration instantanée *est* activée.

  — Si le fichier de contrôle Oracle8i/9i, les journaux de rétablissement en ligne et le fichier SPFILE Oracle9i résident sur le **même** groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle8i/9i, la restauration instantanée *n'est pas* activée. Vous pouvez l'activer en définissant les variables `omnirc` `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Pour plus d'informations, reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

  Les fichiers journaux de rétablissement archivés ne doivent pas nécessairement résider sur une baie de disques.

- L'utilisateur `ora<ORACLE_SID>` doit être créé sur le système d'application dans le groupe principal `dba`.

  Sur les systèmes UNIX, l'utilisateur UNIX `<ORACLE_SID>adm` doit être créé sur le système d'application dans le groupe UNIX `sapsys`.

- Le logiciel SAP R/3 doit être correctement installé sur le système d'application.

  Les répertoires standard suivants doivent être installés sur le système d'application après l'installation de SAP R/3 :

REMARQUE L'emplacement des répertoires dépend des variables d'environnement (systèmes UNIX) ou de registre (systèmes Windows). Reportez-vous à la documentation SAP R/3 pour plus d'informations.

<ORACLE_HOME>/dbs (systèmes UNIX)
<ORACLE_HOME>\database (systèmes Windows) - les profils Oracle et SAP

<ORACLE_HOME>/bin (systèmes UNIX)
<ORACLE_HOME>\bin (systèmes Windows) - les fichiers binaires Oracle

<SAPDATA_HOME>/sapbackup (systèmes UNIX)
<SAPDATA_HOME>\sapbackup (Systèmes Windows) - le répertoire SAPBACKUP contenant les fichiers journaux BRBACKUP

<SAPDATA_HOME>/sapbarch (systèmes UNIX)
<SAPDATA_HOME>\sapbarch (systèmes Windows) - le répertoire SAPARCH avec fichiers journaux BRARCHIVE

<SAPDATA_HOME>/sapreorg (systèmes UNIX)
<SAPDATA_HOME>\sapreorg (systèmes Windows)

<SAPDATA_HOME>/sapcheck (systèmes UNIX)
<SAPDATA_HOME>\sapcheck (systèmes Windows)

<SAPDATA_HOME>/saptrace (systèmes UNIX)
<SAPDATA_HOME>\saptrace (systèmes Windows)

/usr/sap/*<ORACLE_SID>*/SYS/exe/run (systèmes UNIX)
BRTOOLS (systèmes Windows)

Systèmes UNIX Sur les systèmes UNIX, si les six derniers répertoires ne sont pas aux emplacements indiqués ci-dessus, créez les liens appropriés vers eux.

Sur les systèmes UNIX, le propriétaire du répertoire /usr/sap/*<ORACLE_SID>*/SYS/exe/run doit être l'utilisateur UNIX ora*<ORACLE_SID>*. Le propriétaire des fichiers SAP R/3 doit être l'utilisateur UNIX ora*<ORACLE_SID>* et le groupe UNIX dba avec le bit setuid à 1 (chmod 4755 ...). L'exception est le fichier BRRESTORE, dont le propriétaire doit être l'utilisateur UNIX *<ORACLE_SID>*adm.

Exemple UNIX

Si *<ORACLE_SID>* est PROD, les droits à l'intérieur du répertoire `/usr/sap/<ORACLE_SID>/SYS/exe/run` doivent ressembler à ce qui suit :

```
-rwsr-xr-x   1 oraprod dba 4598276 Apr 17  1998 brarchive
-rwsr-xr-x   1 oraprod dba 4750020 Apr 17  1998 brbackup
-rwsr-xr-x   1 oraprod dba 4286707 Apr 17  1998 brconnect
-rwsr-xr-x   1 prodadm sapsys 430467 Apr 17  1998
brrestore
-rwsr-xr-x   1 oraprod dba 188629 Apr 17  1998 brtools
-rwsr-xr-x   1 oraprod dba 6081400 May  8  1998 sapdba.
```

Systèmes Windows

Sur les systèmes Windows, le partage `SAPMNT` doit être créé sur le système d'application et doit contenir le sous-répertoire *<SAPDATA_HOME>*.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez SAP R/3 BRTOOLS sur le système d'application.
2. Installez les logiciels d'intégration Data Protector.

   Sur les systèmes Windows, les composants logiciels de Data Protector doivent être installés avec le compte administrateur SAP R/3, et ce groupe doit être inclus dans le groupe local `ORA_DBA` ou `ORA_<SID>_DBA` sur le système où l'instance SAP R/3 est exécutée.

   Installez les composants logiciels Data Protector suivants :

   - `Agent HP StorageWorks VA` - sur le système d'application et le système de sauvegarde
   - `Intégration SAP R/3` - sur le système d'application uniquement
   - `Agent de disque` - sur le système d'application et le système de sauvegarde

Intégration HP StorageWorks VA avec Microsoft Exchange Server

Condition préalable

La base de données Microsoft Exchange Server doit être installée sur les volumes source du système d'application. Les objets suivants doivent se trouver sur les volumes source :

- Banque d'informations Microsoft (MIS)
- Service gestionnaire de clés (KMS, facultatif)

- Service de réplication de sites (SRS, facultatif)

Pour pouvoir sauvegarder des journaux de transactions, désactivez l'enregistrement circulaire sur le serveur Microsoft Exchange.

Procédure d'installation

Installez les composants logiciels Data Protector suivants :

- `Agent HP StorageWorks VA` - sur le système d'application et le système de sauvegarde
- `Intégration MS Exchange 2000/2003` - sur le système d'application uniquement

Intégration HP StorageWorks VA avec Microsoft SQL Server

Condition préalable

Microsoft SQL Server doit être installé sur le système d'application. Les bases de données utilisateur *doivent* se trouver sur les volumes source en baie de disques, tandis que les bases de données système peuvent être installées n'importe où. Cependant, si les bases de données système sont elles aussi installées sur la baie de disques, elles *doivent* l'être sur des volumes source *différents* de ceux des bases de données utilisateur.

Procédure d'installation

Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :

- `Agent HP StorageWorks VA`
- `Intégration MS SQL 7.0/2000`

Intégration de HP StorageWorks Enterprise Virtual Array

Pour intégrer HP StorageWorks EVA à Data Protector, installez les composants logiciels HP Data Protector suivants sur le système d'application et le système de sauvegarde :

- `Agent HP StorageWorks EVA SMI-S`
- `Agent général de supports`

  Installez le composant `Agent général de supports` sur le système de sauvegarde pour sauvegarder les données en bloc. Installez-le sur le système d'application pour sauvegarder les journaux d'archive ou pour restaurer le système.

- `Agent de disque`

  Installez le composant `Agent de disque` sur les systèmes d'application et de sauvegarde pour exécuter des sauvegardes ZDB d'image disque et de système de fichiers. Les clients sans Agent de disque ne sont pas répertoriés dans les listes déroulantes `Système d'application` et `Système de sauvegarde` lors de la création d'une spécification ZDB.

Installation sur un cluster

Vous pouvez installer l'intégration HP StorageWorks EVA dans un environnement de cluster. Pour connaître les configurations de clusters prises en charge et la configuration requise pour l'installation, reportez-vous au *Guide de l'administrateur HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

Intégration à d'autres applications

Si vous souhaitez installer l'intégration HP StorageWorks EVA avec une application de base de données, installez le composant Data Protector spécifique à l'intégration de cette application sur les systèmes d'application et de sauvegarde, et effectuez les tâches spécifiques à cette intégration. Vous pouvez installer l'intégration HP StorageWorks EVA avec Oracle, SAP R/3, Microsoft Exchange Server et Microsoft SQL Server et Microsoft VSS.

Intégration HP StorageWorks EVA avec Oracle

Configuration système requise

- Les logiciels Oracle suivants doivent être installés sur les volumes sources du système d'application :

  ✓ Oracle Enterprise Server (RDBMS)

  ✓ Logiciel Oracle Net8

  ✓ SQL*Plus

  Il est nécessaire d'installer au moins Oracle Server et SQL*NET V2 ou NET8.

- Les fichiers de base de données Oracle du système d'application doivent être installés sur les volumes source qui seront dupliqués à l'aide de l'agent SMI-S que vous avez installé.

Selon l'emplacement du fichier de contrôle Oracle, des fichiers journaux de rétablissement en ligne et du fichier SPFILE Oracle9i/10g, les deux options suivantes sont possibles :

— Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE Oracle9i/10g résident sur un groupe de volumes (si LVM est utilisé) ou un volume source **différent** des fichiers de données Oracle.

La restauration instantanée est activée par défaut dans ce type de configuration.

— Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE Oracle9i/10g résident sur le **même** groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle.

Par défaut, la restauration instantanée *n'est pas* activée dans ce type de configuration. Vous pouvez l'activer en définissant les variables `omnirc ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Pour plus d'informations, reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

Les fichiers journaux de rétablissement archivés Oracle ne doivent pas nécessairement résider sur des volumes source.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez la base de données du catalogue de récupération Oracle.

   Reportez-vous à la documentation Oracle pour obtenir des informations sur l'installation de la base de données du catalogue de récupération Oracle sur le système d'application. Laissez le catalogue de récupération non enregistré.

2. Installez les composants logiciels Data Protector suivants :

   - `Agent HP StorageWorks EVA SMI-S` à la fois sur le système d'application et le système de sauvegarde.
   - `Intégration Oracle` - si vous souhaitez utiliser la méthode de jeu de sauvegardes ZDB, installez ce composant à la fois sur le système d'application et sur le système de sauvegarde ; si vous souhaitez utiliser la méthode proxy-copy ZDB, installez-le sur le système d'application seulement.

Intégration de HP StorageWorks EVA avec SAP R/3

Configuration système requise

- Les logiciels Oracle suivants doivent être installés sur les volumes source du système d'application.

  ✓ Oracle Enterprise Server (RDBMS)

  ✓ Logiciel Oracle Net8

  ✓ SQL*Plus

  Il est nécessaire d'installer au moins RDBMS et SQL*NET V2 ou NET8.

- La base de données du système d'application peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers. Les fichiers de données Oracle *doivent* résider sur des volumes source en baie de disques.

  Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas nécessairement résider sur une baie de disques.

  Pour la *sauvegarde hors ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* résider sur une baie de disques. Toutefois, notez les points suivants :

  — Si le fichier de contrôle Oracle8i/9i, les journaux de rétablissement en ligne et le fichier SPFILE Oracle9i résident sur un groupe de volumes (si LVM est utilisé) ou un volume source **différent** des fichiers de données Oracle8i/9i, la restauration instantanée *est* activée.

  — Si le fichier de contrôle Oracle8i/9i, les journaux de rétablissement en ligne et le fichier SPFILE Oracle9i résident sur le **même** groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle8i/9i, la restauration instantanée *n'est pas* activée. Vous pouvez l'activer en définissant les variables `omnirc` `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Pour plus d'informations, reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

  Les fichiers journaux de rétablissement archivés ne doivent pas nécessairement résider sur une baie de disques.

- L'utilisateur `ora<ORACLE_SID>` doit être créé sur le système d'application dans le groupe principal `dba`.

  Sur les systèmes UNIX, l'utilisateur UNIX `<ORACLE_SID>adm` doit être créé sur le système d'application dans le groupe UNIX `sapsys`.

- Le logiciel SAP R/3 doit être correctement installé sur le système d'application.

  Les répertoires standard suivants doivent être installés sur le système d'application après l'installation de SAP R/3 :

REMARQUE L'emplacement des répertoires dépend des variables d'environnement (systèmes UNIX) ou de registre (systèmes Windows). Reportez-vous à la documentation SAP R/3 pour plus d'informations.

`<ORACLE_HOME>/dbs` (systèmes UNIX)
`<ORACLE_HOME>\database` (systèmes Windows) - les profils Oracle et SAP

`<ORACLE_HOME>/bin` (systèmes UNIX)
`<ORACLE_HOME>\bin` (systèmes Windows) - les fichiers binaires Oracle

`<SAPDATA_HOME>/sapbackup` (systèmes UNIX)
`<SAPDATA_HOME>\sapbackup` (systèmes Windows) - le répertoire SAPBACKUP avec fichiers journaux BRBACKUP

`<SAPDATA_HOME>/sapbarch` (systèmes UNIX)
`<SAPDATA_HOME>\sapbarch` (systèmes Windows) - le répertoire SAPARCH avec fichiers journaux BRARCHIVE

`<SAPDATA_HOME>/sapreorg` (systèmes UNIX)
`<SAPDATA_HOME>\sapreorg` (systèmes Windows)

`<SAPDATA_HOME>/sapcheck` (systèmes UNIX)
`<SAPDATA_HOME>\sapcheck` (systèmes Windows)

`<SAPDATA_HOME>/saptrace` (systèmes UNIX)
`<SAPDATA_HOME>\saptrace` (systèmes Windows)

`/usr/sap/<ORACLE_SID>/SYS/exe/run` (systèmes UNIX)
BRTOOLS (systèmes Windows)

Systèmes UNIX

Sur les systèmes UNIX, si les six derniers répertoires ne sont pas aux emplacements indiqués ci-dessus, créez les liens appropriés vers eux.

Sur les systèmes UNIX, le propriétaire du répertoire `/usr/sap/<ORACLE_SID>/SYS/exe/run` doit être l'utilisateur UNIX `ora<ORACLE_SID>`. Le propriétaire des fichiers SAP R/3 doit être l'utilisateur UNIX `ora<ORACLE_SID>` et le groupe UNIX `dba` avec le bit setuid à 1 (chmod 4755 ...). L'exception est le fichier BRRESTORE, dont le propriétaire doit être l'utilisateur UNIX `<ORACLE_SID>adm`.

Exemple UNIX

Si `<ORACLE_SID>` est PROD, les droits à l'intérieur du répertoire `/usr/sap/<ORACLE_SID>/SYS/exe/run` doivent ressembler à ce qui suit :

```
-rwsr-xr-x   1 oraprod dba 4598276 Apr 17  1998 brarchive
-rwsr-xr-x   1 oraprod dba 4750020 Apr 17  1998 brbackup
-rwsr-xr-x   1 oraprod dba 4286707 Apr 17  1998 brconnect
-rwsr-xr-x   1 prodadm sapsys 430467 Apr 17  1998
brrestore
-rwsr-xr-x   1 oraprod dba 188629 Apr 17  1998 brtools
-rwsr-xr-x   1 oraprod dba 6081400 May  8  1998 sapdba.
```

Systèmes Windows

Sur les systèmes Windows, le partage `SAPMNT` doit être créé sur le système d'application et doit contenir le sous-répertoire `<SAPDATA_HOME>`.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez SAP R/3 BRTOOLS sur le système d'application.
2. Installez les logiciels d'intégration Data Protector.

   Sur les systèmes Windows, les composants logiciels de Data Protector doivent être installés avec le compte administrateur SAP R/3, et ce groupe doit être inclus dans le groupe local `ORA_DBA` ou `ORA_<SID>_DBA` sur le système où l'instance SAP R/3 est exécutée.

   Installez les composants logiciels Data Protector suivants :

   - `Agent HP StorageWorks EVA SMI-S` à la fois sur le système d'application et le système de sauvegarde.
   - `Intégration SAP R/3` - sur le système d'application uniquement.
   - `Agent de disque` - sur le système d'application et le système de sauvegarde.

Intégration HP StorageWorks EVA avec Microsoft Exchange Server

Condition préalable

La base de données Microsoft Exchange Server doit être installée sur les volumes sources du système d'application. Les objets suivants doivent se trouver sur les volumes sources :

- Banque d'informations Microsoft (MIS)
- Service gestionnaire de clés (KMS, facultatif)
- Service de réplication de sites (SRS, facultatif)

Pour pouvoir sauvegarder des journaux de transactions, désactivez l'enregistrement circulaire sur le serveur Microsoft Exchange.

Procédure d'installation

Installez les composants logiciels Data Protector suivants :

- `Agent HP StorageWorks EVA SMI-S` à la fois sur le système d'application et le système de sauvegarde.
- `Intégration MS Exchange 2000/2003` - sur le système d'application uniquement.

Intégration HP StorageWorks EVA avec MS SQL

Condition préalable

Microsoft SQL Server doit être installé sur le système d'application. Les bases de données utilisateur *doivent* se trouver sur les volumes source en baie de disques, tandis que les bases de données système peuvent être installées n'importe où. Cependant, si les bases de données système sont elles aussi installées sur la baie de disques, elles *doivent* l'être sur des volumes sources *différents* de ceux des bases de données utilisateur.

Procédure d'installation

Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :

- `Agent HP StorageWorks EVA SMI-S` à la fois sur le système d'application et le système de sauvegarde
- `Intégration MS SQL 7.0/2000`

Installation de l'interface utilisateur localisée de Data Protector

Data Protector A.06.00 dispose d'une interface graphique utilisateur localisée de Data Protector sur les systèmes Windows et UNIX. Elle se compose de l'interface graphique utilisateur et de l'interface de ligne de commande de Data Protector localisées. L'aide en ligne et la documentation papier sont également disponibles en version localisée. Pour savoir quels sont les manuels Data Protector localisés, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

REMARQUE

Le support de langue anglais est installé par défaut pendant l'installation de Data Protector. Lorsque vous installez un support de langue supplémentaire, l'interface utilisateur localisée de Data Protector démarre en fonction de l'environnement local paramétré sur le système.

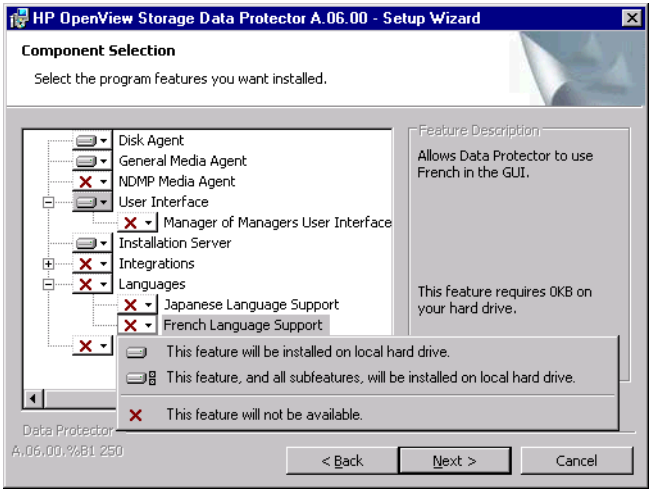
Installation de l'interface utilisateur localisée de Data Protector sur les systèmes Windows

Installation en local

Pour installer l'interface utilisateur localisée de Data Protector sur des systèmes Windows, sélectionnez le support de langue approprié (français ou japonais) dans la page `Installation personnalisée` de l'assistant d'`installation`, comme indiqué à la figure 2-21.

Pour connaître la procédure d'installation en local, reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d’installation (IS) de Data Protector” à la page 19.

Figure 2-21 Sélection du support de langue lors de l'installation

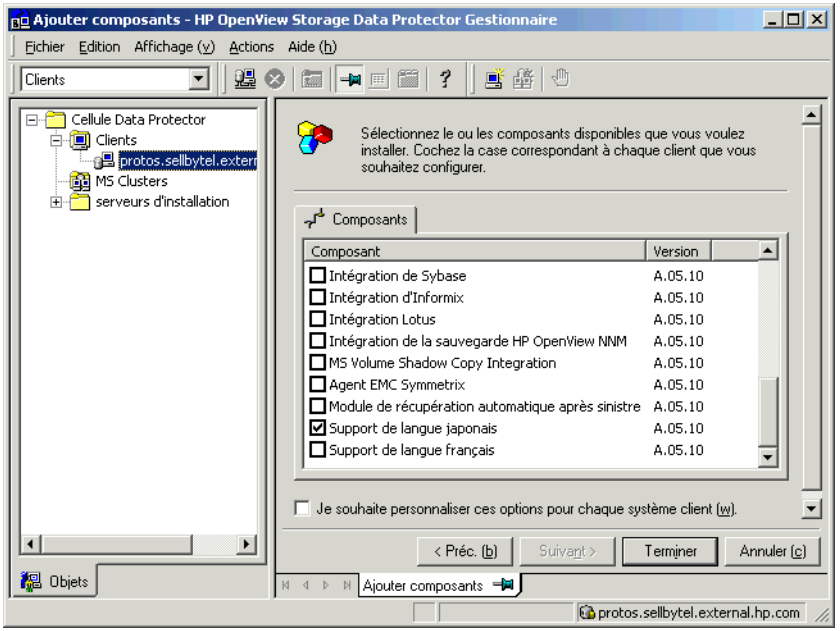


Installation à distance

Lors de la distribution à distance du support de langue de Data Protector à l'aide du Serveur d'installation, sélectionnez le support de langue approprié dans la page `Sélection des composants` de l'assistant `Ajouter composants`, comme indiqué à la figure 2-22.

Pour connaître la procédure pour ajouter à distance des composants logiciels Data Protector à des clients, reportez-vous à la section “Installation distante de clients Data Protector” à la page 54.

Figure 2-22 **Installation à distance du support de langue**



Installation de l'interface utilisateur localisée de Data Protector sur les systèmes UNIX

Installation en local

Vous pouvez installer en local le support de langue japonais ou français uniquement sur un client Data Protector à l'aide de la commande `omnisetup.sh`. Spécifiez le composant logiciel `jpn_ls` ou `fra_ls`, en fonction du support de langue dont vous avez besoin. Pour connaître la procédure détaillée, reportez-vous à la section “Installation locale de clients UNIX” à la page 130.

Si vous utilisez l'utilitaire `swinstall`, `pkgadd` ou `rpm` pour installer le Gestionnaire de cellule ou le Serveur d’installation de Data Protector, vous ne pouvez installer que le support de langue anglais. Si vous souhaitez que l'interface utilisateur localisée de Data Protector réside sur le même système que le Gestionnaire de cellule ou le Serveur d’installation, vous devez installer le support de langue supplémentaire à distance.

Installation à distance

Lors de la distribution à distance du support de langue de Data Protector à l'aide du Serveur d'installation, sélectionnez le support de langue approprié dans la page `Sélection des composants` de l'assistant `Ajouter composants`, comme indiqué à la figure 2-22.

Pour connaître la procédure pour ajouter à distance des composants logiciels Data Protector à des clients, reportez-vous à la section “Installation distante de clients Data Protector” à la page 54.

Dépannage

Si l'interface utilisateur de Data Protector en anglais démarre après que vous avez installé un support de langue différent, effectuez les vérifications suivantes :

1. Assurez-vous que les fichiers suivants existent :

   Pour le support de langue français :

   - Sous Windows : `<répertoire_Data_Protector>\bin\OmniFra.dll`
   - Sous HP-UX : `/opt/omni/lib/nls/fr.iso88591/omni.cat`
   - Sous Solaris : `/opt/omni/lib/nls/fr.ISO8859-1/omni.cat`

   Pour le support de langue japonais :

   - Sous Windows : `<répertoire_Data_Protector>\bin\OmniJpn.dll`
   - Sous HP-UX : `/opt/omni/lib/nls/ja.eucJP/omni.cat` et `/opt/omni/lib/nls/ja.SJIS/omni.cat`
   - Sous Solaris : `/opt/omni/lib/nls/ja.eucJP/omni.cat` et `/opt/omni/lib/nls/ja.PCK/omni.cat`

2. Vérifiez les paramètres régionaux sur votre système :

   - Sous Windows : dans le `Panneau de configuration` de Windows, cliquez sur `Options régionales` et vérifiez que la langue sélectionnée dans les paramètres régionaux et de langue est appropriée.

- Sous UNIX : exécutez la commande suivante pour configurer les paramètres régionaux :

  ```
  export LANG=<langue>
  locale
  ```

  où *<langue>* représente le paramètre régional dans le format suivant : `langue[_région].jeu de code`.

  Par exemple, `ja_JP.eucJP`, `ja_JP.SJIS` ou `ja_JP.PCK` pour le paramètre régional japonais et `fr_FR.iso88591` pour le paramètre régional français. Notez que la partie jeu de code de la variable `LANG` est obligatoire et doit correspondre à la partie jeu de code du nom du répertoire apparenté.

Installation de l'Edition serveur unique de Data Protector

L'Edition serveur unique (SSE) de Data Protector est conçue pour les environnements restreints dans lesquels les sauvegardes s'exécutent sur un seul périphérique connecté à un Gestionnaire de cellule. Elle est disponible pour les plates-formes Windows prises en charge ainsi que pour les plates-formes HP-UX et Solaris.

Pour installer le Gestionnaire de cellule et (le cas échéant) le Serveur d'installation, suivez les instructions figurant dans la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 19.

Limites

Lorsque vous examinez la licence de l'Edition serveur unique, tenez compte des limites suivantes :

Limites de l'Edition serveur unique pour Windows

- L'Edition serveur unique prend en charge les sauvegardes vers un seul périphérique à la fois, lequel est connecté à un seul Gestionnaire de cellule.
- Elle ne prend en charge qu'un changeur automatique DDS à 10 emplacements.
- Elle ne prend en charge ni les clients, ni les serveurs UNIX (et HP-UX). Si vous essayez d'effectuer une sauvegarde sur une machine UNIX, la session est abandonnée.
- Si une cellule contient un Gestionnaire de cellule Windows, vous ne pouvez sauvegarder que des clients Windows. L'Edition serveur unique ne prend pas en charge la sauvegarde vers les clients Novell NetWare.
- L'ajout de produits d'extension n'est pas pris en charge par l'Edition serveur unique.
- La gestion de clusters n'est pas prise en charge par l'Edition serveur unique.
- La récupération après sinistre n'est pas prise en charge.

Le nombre de clients Windows n'est pas limité.

Pour connaître les périphériques pris en charge, reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

Limites de l'Edition serveur unique pour HP-UX et Solaris

- L'Edition serveur unique prend en charge les sauvegardes vers un seul périphérique à la fois, lequel est connecté à un seul Gestionnaire de cellule.
- Elle ne prend en charge qu'un changeur automatique DDS à 10 emplacements.
- Sur un Gestionnaire de cellule UNIX, vous ne pouvez pas sauvegarder des serveurs, mais seulement des clients UNIX, des clients Windows, des clients Solaris et des clients Novell NetWare.
- L'ajout de produits d'extension n'est pas pris en charge par l'Edition serveur unique.
- La gestion de clusters n'est pas prise en charge par l'Edition serveur unique.

Le nombre de clients (UNIX, Windows) n'est pas limité.

Pour connaître les périphériques pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

Installation d'un mot de passe

Pour obtenir des instructions détaillées sur l'installation d'un mot de passe sur le Gestionnaire de cellule, reportez-vous à la section “Mots de passe Data Protector” à la page 333.

Installation du composant Rapports Web de Data Protector

Le composant Rapports Web de Data Protector est installé par défaut avec d'autres composants Data Protector et à ce titre, vous pouvez l'utiliser en local à partir de votre système.

Vous pouvez également l'installer sur un serveur Web et ainsi le rendre disponible sur les autres systèmes, sur lesquels l'installation des composants logiciels Data Protector n'est pas obligatoire.

Configuration système requise

Pour utiliser la génération de rapports Web de Data Protector sur votre système, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector* pour connaître la configuration requise et les limites.

Installation

Procédez comme suit pour installer le composant Rapports Web Data Protector sur un serveur Web :

1. Copiez les fichiers de rapport Java Data Protector suivants sur le serveur. Il n'est pas nécessaire que le serveur soit un client Data Protector.

   - Sur les systèmes Windows disposant de l'interface utilisateur Data Protector, les fichiers se trouvent dans le répertoire suivant :

     `<répertoire_Data_Protector>\java\bin`

   - Sur un système UNIX disposant de l'interface utilisateur Data Protector, les fichiers se trouvent dans le répertoire suivant :

     `/opt/omni/java/bin`

2. Ouvrez le fichier `WebReporting.html` dans votre navigateur pour accéder aux Rapports Web de Data Protector.

   Vous devez rendre le fichier disponible aux utilisateurs des Rapports Web sous forme d'URL complète. Par exemple, vous pouvez placer un lien vers ce fichier à partir de votre site Intranet.

CONSEIL Aucun mot de passe n'est requis par défaut pour utiliser les Rapports Web Data Protector. Vous pouvez cependant en indiquer un et restreindre ainsi l'accès aux Rapports Web. Pour connaître la procédure à suivre, reportez-vous à l'index de l'aide en ligne (rubrique "rapports Web, restriction d'accès").

Etape suivante Une fois l'installation terminée, reportez-vous à l'index de l'aide en ligne (rubrique "interface de génération de rapports Web, configuration de notifications") pour plus d'informations sur les questions de configuration et la création de rapports personnalisés.

Installation de Data Protector sur MC/ServiceGuard

Data Protector prend en charge MC/ServiceGuard (MC/SG) pour HP-UX et Linux. Pour obtenir des informations détaillées sur les versions de systèmes d'exploitation prises en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

Si votre Gestionnaire de cellule doit être compatible cluster, notez que l'adresse IP du serveur virtuel doit être utilisée pour les licences.

Installation d'un Gestionnaire de cellule compatible cluster

Configuration système requise

Avant d'installer un Gestionnaire de cellule Data Protector sur MC/ServiceGuard, vérifiez les éléments suivants :

- ✓ Décidez quels systèmes seront les Gestionnaires de cellule principal et secondaire. Ils doivent tous être équipés de MC/ServiceGuard et configurés en tant que membres du cluster.
- ✓ Le Gestionnaire de cellule Data Protector doté des correctifs recommandés, ainsi que tous les autres composants logiciels Data Protector des intégrations que vous souhaitez intégrer au cluster doivent être installés sur le nœud principal et sur chaque nœud secondaire.

  La procédure d'installation est la procédure standard d'installation du système du Gestionnaire de cellule. Reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d’installation (IS) de Data Protector” à la page 19.

Etape suivante

Une fois l'installation terminée, vous devez configurer les Gestionnaires de cellule principal et secondaire, ainsi que le package de Gestionnaire de cellule. Reportez-vous à l'index de l'aide en ligne (rubrique "cluster, MC/ServiceGuard") pour plus d'informations sur la configuration de MC/ServiceGuard avec Data Protector.

Installation d'un client compatible cluster

IMPORTANT Les clients Data Protector compatibles cluster doivent être installés sur tous les nœuds de clusters.

La procédure d'installation est la procédure standard d'installation de Data Protector sur un client UNIX. Pour connaître la procédure détaillée, reportez-vous aux sections “Installation de clients HP-UX” à la page 74 et “Installation de clients Linux” à la page 86.

Etape suivante Lorsque vous avez terminé l'installation, vous devez importer le serveur virtuel (nom d'hôte spécifié dans le package de clusters) dans la cellule Data Protector. Reportez-vous à la section “Importation d'un client compatible dans une cellule” à la page 200.

Reportez-vous à l'index de l'aide en ligne (rubrique "configuration") pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration Data Protector.

Installation de Data Protector sur Microsoft Cluster Server

Pour connaître les systèmes d'exploitation pris en charge pour l'intégration de Microsoft Cluster Server, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

Si votre Gestionnaire de cellule doit être compatible clusters, notez que l'adresse IP du serveur virtuel doit être utilisée pour les licences.

Installation d'un Gestionnaire de cellule compatible cluster

Configuration système requise

Avant d'installer le Gestionnaire de cellule compatible cluster, assurez-vous qu'il n'y a pas sur le cluster de ressources portant les noms suivants :

```
OBVS_MCRS,OBVS_VELOCIS,OmniBack_Share
```

S'il en existe, et que vous effectuez une nouvelle installation (pas une mise à niveau), vous devez supprimer ou renommer ces ressources car Data Protector utilise ces noms pour le serveur virtuel Data Protector.

Pour ce faire, procédez comme suit :

1. Cliquez sur `Démarrer` -> `Programmes` -> `Outils d'administration` -> `Administrateur de clusters`.
2. Vérifiez la liste des ressources afin de les supprimer ou de les renommer, le cas échéant.

Pour installer et configurer correctement Data Protector dans un environnement Microsoft Cluster Server, vous devez fournir un compte disposant des droits utilisateur appropriés :

✓ Droits d'administrateur sur le Gestionnaire de cellule

✓ Droits administrateur de clusters dans le cluster

✓ Le mot de passe n'expire jamais

✓ Connexion comme un service

- ✓ L'utilisateur ne peut pas changer de mot de passe
- ✓ Tous les horaires d'accès sont autorisés

REMARQUE Lorsque vous installez un Gestionnaire de cellule Data Protector en tant qu'élément compatible cluster dans un environnement Microsoft Cluster, le compte utilisateur Data Protector doit être un compte d'utilisateur du domaine disposant de tous les droits mentionnés ci-dessus.

CONSEIL Pour installer un serveur de clusters, vous devez disposer d'un compte doté de droits d'administrateur sur tous les systèmes de clusters. Il est recommandé d'utiliser également ce compte pour installer Data Protector. Des droits utilisateur incorrects peuvent entraîner l'exécution de services Data Protector en mode standard au lieu du mode compatible cluster.

Avant d'installer le logiciel du Gestionnaire de cellule sur un cluster, vérifiez les éléments suivants :

- ✓ Un cluster doit être installé correctement avec la totalité de ses fonctions. Par exemple, vous devez pouvoir déplacer des groupes d'un nœud à l'autre autant de fois que cela est nécessaire, et ce sans aucun problème de disque partagé.
- ✓ Un groupe au moins dans le cluster doit disposer d'une ressource de *<partage de fichier>* définie. Data Protector installera ses composants base de données dans cette ressource de *<partage de fichier>*. Reportez-vous à la documentation spécifique aux clusters pour savoir comment définir une ressource de *<partage de fichier>*. Notez que le nom de *<partage de fichier>* de cette ressource ne peut pas être `OmniBack`.
- ✓ Soit le serveur virtuel n'existe pas dans le même groupe en tant que groupe de ressources de *<partage de fichier>*, soit vous devez créer un serveur virtuel en utilisant une adresse IP libre enregistrée et en lui associant un nom de réseau.
- ✓ La ressource de *<partage de fichier>* dans laquelle Data Protector sera installé doit disposer d'une `adresse IP`, d'un `nom de réseau` et d'un ensemble de `disques physiques` parmi les dépendances du

<partage de fichier>. Cela est nécessaire pour s'assurer que le groupe de clusters Data Protector pourra s'exécuter sur n'importe quel nœud, indépendamment de tout autre groupe.

- ✓ Vérifiez que seul l'administrateur de clusters a accès à la ressource de *<partage de fichier>* et qu'il dispose d'un accès complet.
- ✓ Chaque système du cluster doit être en cours d'exécution.
- ✓ Si le logiciel Data Protector est installé sur un système du cluster, vous devez le désinstaller avant de procéder à l'installation. L'option de mise à niveau est prise en charge uniquement si le logiciel Data Protector déjà installé est le Gestionnaire de cellule compatible cluster.
- ✓ Data Protector doit être installé au même emplacement (lecteur et chemin d'accès) sur tous les nœuds cluster. Assurez-vous que ces emplacements sont libres.
- ✓ Les autres installations basées sur MSI *ne* doivent *pas* s'exécuter sur d'autres noeuds cluster.

Installation en local

Vous devez installer en local, à partir du DVD-ROM, le logiciel du Gestionnaire de cellule Data Protector compatible cluster. Pour ce faire, procédez comme suit :

1. Insérez le DVD-ROM d'installation Windows et exécutez :

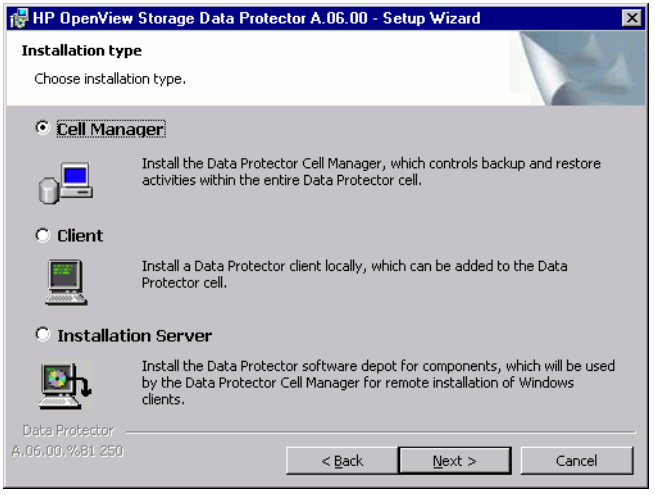
   Systèmes 32 bits : `\Windows_other\i386\setup.exe`

   Systèmes 64 bits : `\Windows_other\x8664\setup.exe`

   L'assistant d'installation de Data Protector s'affiche.

2. Suivez les instructions de l'assistant et lisez attentivement le contrat de licence. Si vous en acceptez les termes, cliquez sur `Suivant` pour continuer.
3. Dans la page `Type d'installation`, sélectionnez `Gestionnaire de cellule`, puis cliquez sur `Suivant` pour installer le logiciel Gestionnaire de cellule de Data Protector.

Figure 2-23 Sélection du type d'installation



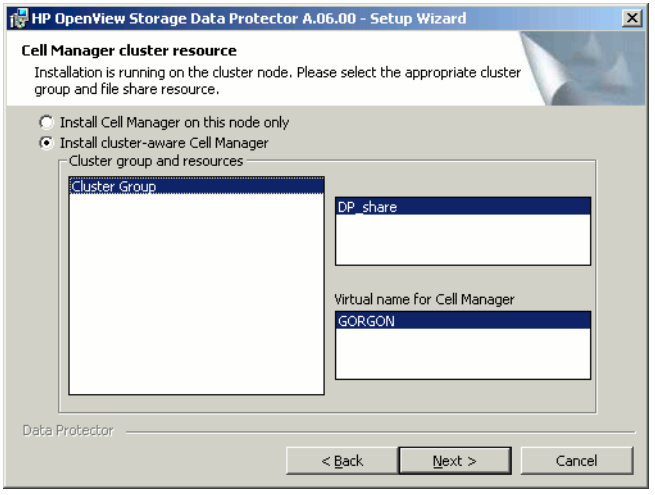
4. Le processus d'installation détecte automatiquement qu'il fonctionne dans un environnement de clusters. Sélectionnez `Install cluster-aware Cell Manager (Installation du Gestionnaire de cellule compatible cluster)` pour activer la configuration d'un cluster.

   Sélectionnez le groupe de clusters, le nom d'hôte virtuel et la ressource de *`<partage de fichier>`* du cluster sur laquelle résideront les fichiers Data Protector partagés et la base de données.

REMARQUE

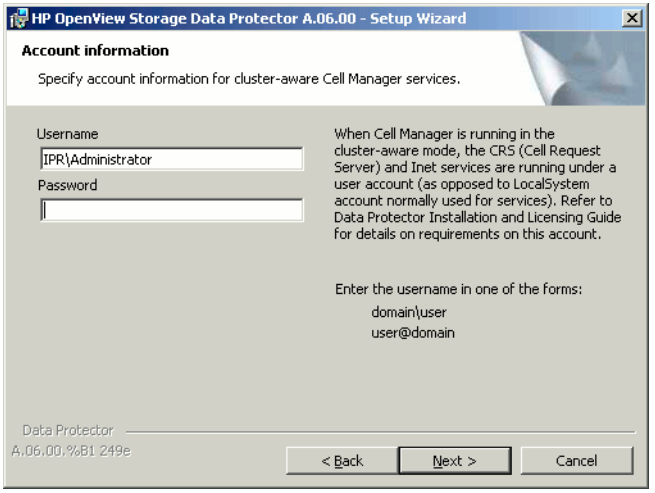
Si vous sélectionnez `Install Cell Manager on this node only (Installer le Gestionnaire de cellule sur ce noeud uniquement)`, le Gestionnaire de cellule *ne* sera *pas* compatible cluster. Reportez-vous à la section “Installation d'un Gestionnaire de cellule Windows” à la page 31.

Figure 2-24 Sélection de la ressource de cluster



5. Saisissez le nom d'utilisateur et le mot de passe correspondant au compte qui sera utilisé pour lancer les services Data Protector.

Figure 2-25 Saisie des informations relatives au compte



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

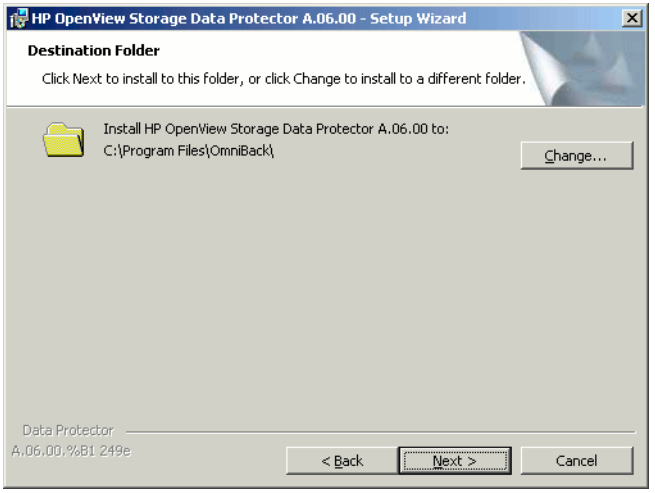
   Sinon, cliquez sur `Modifier` pour ouvrir la fenêtre `Modifier le dossier de destination actuel` et entrez un autre chemin.

7. Dans la fenêtre `Sélection des composants`, sélectionnez les composants que vous souhaitez installer sur tous les nœuds cluster et les serveurs virtuels cluster. Cliquez sur `Suivant`.

   Le composant d'intégration MS Cluster est automatiquement sélectionné.

   Les composants sélectionnés seront installés sur tous les noeuds du cluster.

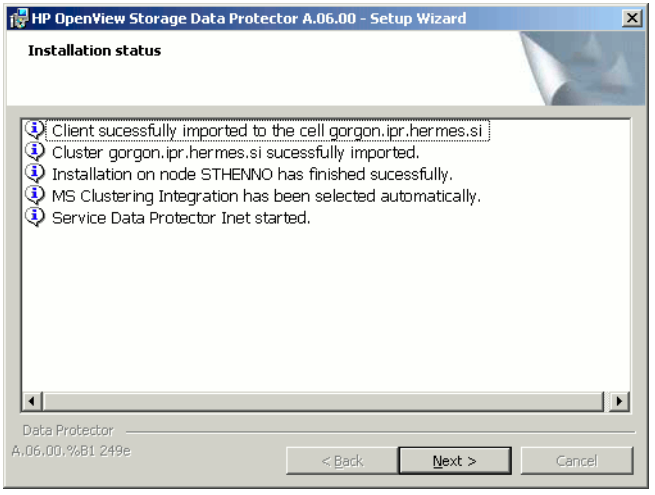
Figure 2-26 Page de sélection des composants



8. La liste des composants sélectionnés s'affiche. Cliquez sur `Installer`.

9. La page `Installation setup (Configuration de l'installation)` s'affiche. Cliquez sur `Suivant`.

Figure 2-27 Page d'état de l'installation



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

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

    Sur les systèmes d'exploitation autres que Windows x64, pour installer ou mettre à niveau l'utilitaire HP OpenView AutoPass, sélectionnez l'option `Start AutoPass installation (Démarrer l'installation d'AutoPass)` ou `Upgrade AutoPass installation (Mettre à niveau l'installation d'AutoPass)`.

    Il *n'*est *pas* recommandé d'installer l'utilitaire HP OpenView AutoPass dans un environnement Microsoft Cluster, car il ne serait installé que sur un seul nœud et non sur tous. Toutefois, si vous installez AutoPass, vous devez désinstaller Data Protector du même noeud sur lequel il était installé, une fois que vous décidez de supprimer Data Protector du système.

    Sur les systèmes d'exploitation Windows x64, AutoPass n'est pas installé.

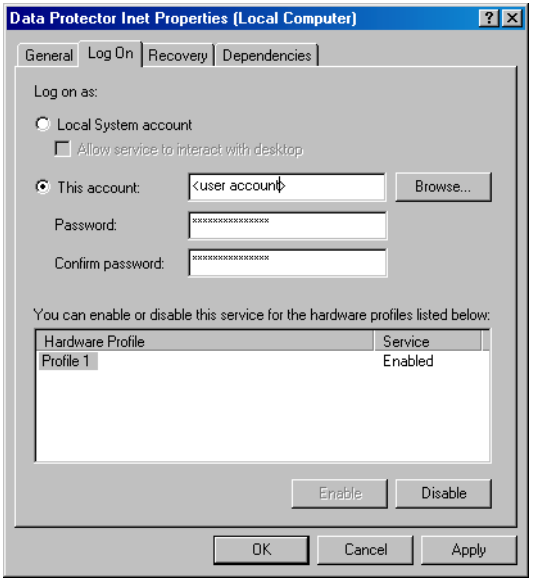
    Cliquez sur `Terminer` pour terminer l'installation.

Vérification de l'installation

Une fois l'installation terminée, vous pouvez vous assurer que le logiciel Data Protector a été installé correctement. Pour ce faire, procédez comme suit :

1. Vérifiez si le compte de service cluster est affecté au service Data Protector `Inet` sur chaque nœud du cluster. Vérifiez que le même utilisateur est également ajouté au groupe d'utilisateurs `Admin` de Data Protector. Le type de compte de connexion défini doit être `Ce compte` comme illustré dans la figure 2-28 à la page 186.

Figure 2-28 Compte utilisateur Data Protector



2. Basculez vers le répertoire `<répertoire_Data_Protector>\bin` et exécutez la commande suivante :

   ```
   omnirsh <hôte> INFO_CLUS
   ```

   où `<hôte>` est le nom du serveur virtuel cluster. Le résultat doit contenir la liste des noms des systèmes se trouvant dans le cluster et le nom du serveur virtuel. Si `0 "NONE"` est affiché, Data Protector n'est pas installé en mode compatible cluster.

3. Lancez l'interface graphique utilisateur de Data Protector, sélectionnez le contexte `Clients`, puis cliquez sur `MS Clusters`. Les systèmes récemment installés doivent apparaître dans la zone de résultats.

Installation d'un client compatible cluster

Configuration système requise

Avant d'installer un client Data Protector compatible cluster, les conditions préalables suivantes doivent être remplies :

- ✓ Un cluster doit être installé correctement avec la totalité de ses fonctionnalités sur tous les nœuds cluster. Par exemple, vous devez pouvoir déplacer des groupes d'un nœud à l'autre autant de fois que cela est nécessaire, et ce sans aucun problème de disque partagé.
- ✓ Chaque système du cluster doit être en cours d'exécution.

Installation en local

Les clients Data Protector compatibles cluster doivent être installés localement, à partir du DVD-ROM, sur chaque nœud cluster. Les nœuds cluster (clients cluster Data Protector) sont importés vers la cellule spécifiée lors du processus d'installation.

Les droits administrateur de clusters sont requis pour effectuer l'installation. Hormis cette exigence, la configuration d'un client cluster est la même que celle d'un client Windows. Le composant Intégration de cluster, sélectionné par défaut lors de l'installation, doit être installé en plus des composants clients Data Protector, tels que les Agents de disque et les Agents de support.

Reportez-vous à la section “Installation de clients Windows” à la page 68 pour savoir comment installer en local un système client Windows Data Protector. Notez que, lors de l'installation, Data Protector signale qu'un cluster a été détecté.

Si vous installez l'intégration Data Protector Oracle, la procédure de configuration doit être effectuée sur tous les nœuds du cluster, ainsi que sur le serveur virtuel hébergeant le groupe de ressources Oracle.

REMARQUE

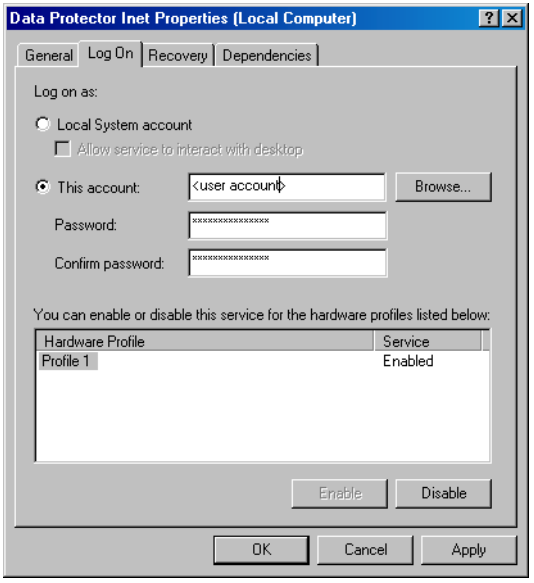
Vous pouvez importer un client compatible cluster dans la cellule Data Protector qui est gérée par le Gestionnaire de cellule standard ou par le Gestionnaire de cellule compatible cluster.

Vérification de l'installation

Une fois l'installation terminée, vous pouvez vous assurer que le logiciel Data Protector a été installé correctement. Pour ce faire, procédez comme suit :

1. Vérifiez si le compte de service cluster est affecté au service Data Protector `Inet` sur chaque nœud du cluster. Vérifiez que le même utilisateur est également ajouté au groupe d'utilisateurs `Admin` de Data Protector. Le type de compte de connexion défini doit être `Ce compte` comme illustré dans la figure 2-28 à la page 186.

Figure 2-29 Compte utilisateur Data Protector



2. Basculez vers le répertoire *<répertoire_Data_Protector>*`\bin`.
3. Exécutez la commande suivante :

   ```
   omnirsh <hôte> INFO_CLUS
   ```

   où *<hôte>* est le nom du système client cluster. Le nom du système client compatible cluster doit apparaître. Si `0 "NONE"` est affiché, Data Protector n'est pas installé en mode compatible cluster.

Veritas Volume Manager

Si Veritas Volume Manager est installé sur le cluster, des étapes supplémentaires sont requises après l'installation de Data Protector sur Microsoft Cluster Server. Pour connaître les opérations supplémentaires à effectuer, reportez-vous à la section “Installation de Data Protector sur Microsoft Cluster avec Veritas Volume Manager” à la page B-84.

Etape suivante

Lorsque vous avez terminé l'installation, vous devez importer le nom d'hôte du serveur virtuel (application compatible cluster) dans la cellule Data Protector. Reportez-vous à la section “Importation d'un client compatible dans une cellule” à la page 200.

Reportez-vous à l'index de l'aide en ligne (rubrique "configuration") pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration Data Protector.

Installation de clients Data Protector sur un cluster Veritas

Il est possible d'installer les clients Data Protector sur des nœuds cluster Veritas, à l'aide d'un Gestionnaire de cellule extérieur au cluster. Si vous utilisez cette configuration, la sauvegarde des disques locaux est prise en charge.

Notez que si vous souhaitez sauvegarder des disques partagés ou des applications compatibles cluster, il faut utiliser l'adresse IP du serveur virtuel pour les licences.

IMPORTANT Pour Data Protector, les sauvegardes compatibles cluster avec basculement ne sont pas prises en charge.

Installation d'un client

La procédure d'installation est identique à la procédure d'installation standard de Data Protector sur un système client Solaris. Pour connaître la procédure détaillée, reportez-vous à la section “Installation de clients Solaris” à la page 79.

Etape suivante Une fois l'installation terminée :

- Si vous souhaitez sauvegarder le serveur virtuel, vous devez l'importer dans la cellule.
- Si vous souhaitez sauvegarder les nœuds physiques, vous devez également les importer dans la cellule.

Reportez-vous à la section “Importation d'un client compatible dans une cellule” à la page 200.

Reportez-vous à l'index de l'aide en ligne (rubrique "configuration") pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration Data Protector.

Installation de clients Data Protector sur un cluster Novell NetWare

Il est possible d'installer les clients Data Protector sur des nœuds cluster Novell NetWare Cluster Services, à l'aide d'un Gestionnaire de cellule extérieur au cluster. Si vous utilisez cette configuration, la sauvegarde des disques locaux, ainsi que la sauvegarde des pools de clusters partagés, sont prises en charge via le serveur virtuel. Pour connaître les systèmes d'exploitation pris en charge pour Microsoft Cluster Server, reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

Notez que si vous souhaitez sauvegarder des disques partagés ou des applications compatibles cluster, il faut utiliser l'adresse IP du serveur virtuel pour les licences.

IMPORTANT Les sauvegardes compatibles cluster avec basculement ne sont pas prises en charge. En cas de basculement, il faut redémarrer manuellement les sessions de sauvegarde ou de restauration.

Dans la mesure où les nœuds cluster contrôlent les périphériques, les périphériques de sauvegarde doivent être configurés sur les nœuds cluster et non sur le serveur virtuel.

Installation d'un client

Avant l'installation Avant d'installer des clients Data Protector sur des nœuds cluster Novell NetWare Cluster Services, il est recommandé de modifier les scripts de déchargement pour *chaque* serveur virtuel présent dans le cluster, afin que l'adresse IP secondaire reste active pendant la migration du serveur virtuel vers un autre nœud. Vous pouvez modifier les scripts de déchargement à l'aide de l'utilitaire Console One de Novell ou de NetWare Remote Manager, conformément à la documentation Novell NetWare.

Exemple

Le script de déchargement par défaut pour chaque serveur virtuel est le suivant :

```
del secondary ipaddress 10.81.1.173
CLUSTER CVSBIND DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
NUDP DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
nss /pooldeactivate=FIRST /overridetype=question
```

Le script de déchargement modifié pour chaque serveur virtuel est le suivant :

```
nss /pooldeactivate=FIRST /overridetype=question
del secondary ipaddress 10.81.1.173
CLUSTER CVSBIND DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
NUDP DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
```

Le script de déchargement modifié commence par démonter et désactiver tous les pools de clusters partagés sur le serveur virtuel ; alors seulement, il supprime l'adresse IP secondaire. Cela signifie que l'adresse IP secondaire reste active pendant la migration.

Pour activer le script de déchargement modifié, mettez le serveur virtuel hors ligne, puis de nouveau en ligne sur le nœud favori.

Modification du script smsrun.bas

Après avoir modifié le(s) script(s) de déchargement, vous devez modifier le script `smsrun.bas` afin d'inclure le chargement du module `TSA600.NLM` (ou `TSAFS.NLM` - selon le module que vous utilisez) avec le paramètre approprié désactivant la prise en charge du cluster. Pour plus d'informations, consultez la rubrique “Known Backup/Restore Issues for NetWare 6.x” (problèmes de sauvegarde/restauration connus pour NetWare 6.x) de la base de données Novell Support Knowledge.

Pour modifier le script `smsrun.bas`, procédez comme suit :

1. Modifiez la protection en écriture du script `SYS:NSN/user/smsrun.bas` en le faisant passer de `lecture seule` à `lecture/écriture`, puis ouvrez-le dans un éditeur standard de la console.
2. Modifiez la ligne `nlmArray = Array(“SMDR”, “TSA600”, “TSAPROXY”)` (ou `nlmArray = Array(“SMDR”, “TSAFS /NoCluster”)`) dans la section `Sub Main()` en indiquant :

   — `nlmArray = Array(“SMDR”, “TSA600 /cluster=off”, “TSAPROXY”)` si `TSA600` est installé.

— `nlmArray = Array("SMDR", "TSAFS /NoCluster")` si `TSAFS` est installé.

Enregistrez les modifications.

3. Sur la console du serveur de fichiers, tapez `SMSSTOP`.
4. Sur la console du serveur de fichiers, tapez `SMSSTART`.

Les volumes partagés du cluster sont désormais visibles pour le module `TSA600.NLM(TSAFS.NLM)`.

Installation

La procédure est identique à celle utilisée pour l'installation standard locale de Data Protector sur un client Novell NetWare. Pour connaître la procédure détaillée, reportez-vous à la section “Installation locale de clients Novell NetWare” à la page 112.

Etape suivante

Une fois l'installation terminée :

- Si vous souhaitez sauvegarder les nœuds physiques, vous devez également les importer dans la cellule.
- Pour sauvegarder le serveur virtuel (volumes partagés du cluster), vous devez l'importer dans la cellule.

Reportez-vous à la section “Importation d'un client compatible dans une cellule” à la page 200.

Reportez-vous à l'index de l'aide en ligne (rubrique "configuration") pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration Data Protector.

3 Gestion de l'installation

Description du chapitre

Ce chapitre décrit les procédures les plus fréquemment effectuées pour modifier la configuration de votre environnement de sauvegarde. Les sections suivantes contiennent des informations relatives aux éléments suivants :

- Comment importer des clients dans une cellule à l'aide de l'interface graphique utilisateur. Reportez-vous à la section “Importation de clients dans une cellule” à la page 197.
- Comment importer un Serveur d’installation dans une cellule à l'aide de l'interface graphique utilisateur. Reportez-vous à la section “Importation d'un Serveur d’installation dans une cellule” à la page 199.
- Comment importer des clusters/serveurs virtuels à l'aide de l'interface graphique utilisateur. Reportez-vous à la section “Importation d'un client compatible dans une cellule” à la page 200.
- Comment exporter des clients à l'aide de l'interface graphique utilisateur. Reportez-vous à la section “Exportation de clients d'une cellule” à la page 204.
- Comment garantir la sécurité à l'aide de l'interface graphique utilisateur. Reportez-vous à la section “Considérations sur la sécurité” à la page 207.
- Comment vérifier quels correctifs Data Protector sont installés. Reportez-vous à la section “Contrôle des correctifs Data Protector installés” à la page 225.
- Comment désinstaller le logiciel Data Protector. Reportez-vous à la section “Désinstallation du logiciel Data Protector” à la page 228.
- Comment ajouter ou supprimer des composants logiciels de Data Protector. Reportez-vous à la section “Changement de composants logiciels Data Protector” à la page 242.

Importation de clients dans une cellule

Lorsque vous distribuez le logiciel Data Protector à des clients à l'aide du Serveur d'installation, les systèmes client sont automatiquement ajoutés à la cellule. Dès que l'installation distante est terminée, le client devient membre de la cellule.

Quand faut-il importer ?

Certains clients, comme Novell NetWare, OpenVMS et Windows XP Edition familiale, doivent être importés dans la cellule après l'installation. **Importer** signifie ajouter manuellement un ordinateur à une cellule une fois le logiciel Data Protector installé. Une fois ajouté à une cellule Data Protector, le système devient un client Data Protector. Dès lors que le système est membre de la cellule, les informations relatives au nouveau client sont écrites dans la base IDB, située dans le Gestionnaire de cellule.

Un client ne peut être membre que d'une cellule. Si vous souhaitez déplacer un client vers une autre cellule, vous devez d'abord l'*exporter* à partir de sa cellule actuelle, puis l'*importer* dans la nouvelle cellule. Pour connaître la procédure à suivre pour exporter des clients, reportez-vous à la section “Exportation de clients d'une cellule” à la page 204.

IMPORTANT

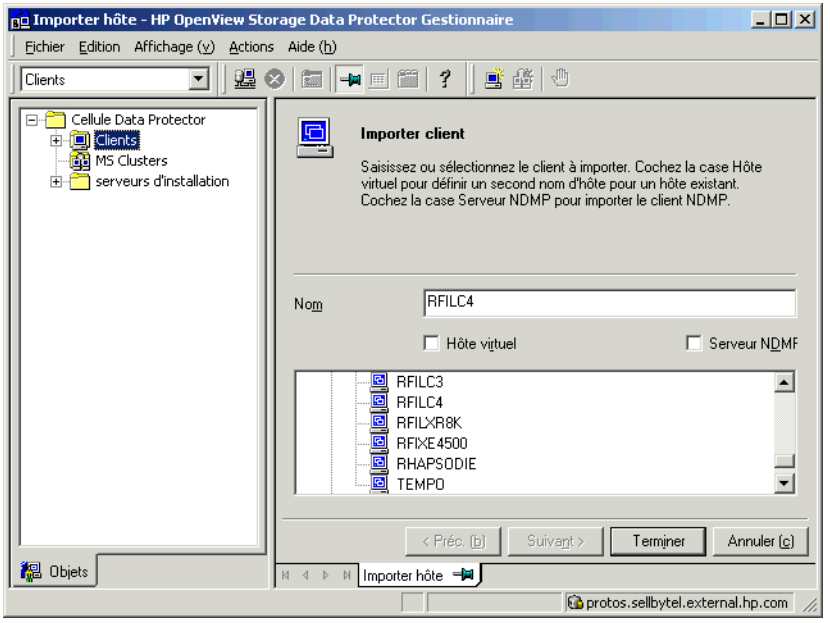
Après avoir installé les clients Data Protector et les avoir importés dans une cellule, il est vivement recommandé de les protéger afin d'empêcher l'accès d'autorités de cellule non autorisées. Reportez-vous à la section “Sécurisation des clients” à la page 210.

Comment importer ?

Vous importez un système client à l'aide de l'interface graphique utilisateur en effectuant les opérations suivantes :

1. Dans le menu contextuel, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur `Clients`, puis cliquez sur `Importer clients`.
3. Saisissez le nom du client ou parcourez le réseau pour sélectionner le client (seulement si vous utilisez une interface graphique Windows) à importer. Reportez-vous à la figure 3-1.

Figure 3-1 Importation d'un client vers la cellule



Si vous importez un client configuré avec plusieurs cartes réseau LAN, sélectionnez l'option `Hôte virtuel`. Avec cette option, vous devez importer tous les noms du même système.

Si vous importez un client NDMP, sélectionnez l'option `Serveur NDMP` et cliquez sur `Suivant`. Spécifiez les informations relatives au serveur NDMP.

Si vous importez un client OpenVMS, saisissez son nom TCP/IP dans la zone de texte `Nom`.

Cliquez sur `Terminer` pour importer le client.

Le nom du client importé s'affiche dans la zone de résultats.

Importation d'un Serveur d'installation dans une cellule

Quand effectuer l'ajout ?

Vous devez ajouter un Serveur d'installation à la cellule dans les cas suivants :

- S'il est installé en tant que Serveur d'installation UNIX indépendant, c'est-à-dire s'il n'est pas installé sur un Gestionnaire de cellule.

  Dans ce cas, il ne sera pas possible d'installer (charger) des clients dans une cellule avant que le Serveur d'installation n'ait été ajouté à cette cellule.

- S'il est installé sur un Gestionnaire de cellule, mais que vous voulez aussi l'utiliser pour effectuer des installations à distance dans une autre cellule. Il doit alors être ajouté dans l'autre cellule (à l'aide de l'interface graphique utilisateur connectée au Gestionnaire de cellule de l'autre cellule).

Contrairement à un client, un Serveur d'installation peut appartenir à plusieurs cellules. Par conséquent, il n'est pas nécessaire de le supprimer d'une cellule (exporter) pour pouvoir l'ajouter à une autre cellule (importer).

Comment effectuer l'ajout ?

Le processus d'importation d'un Serveur d'installation ressemble à celui d'un client. Pour exécuter cette tâche à l'aide de l'interface graphique utilisateur de Data Protector (connectée au Gestionnaire de cellule de la cellule à laquelle le Serveur d'installation doit être ajouté), procédez comme suit :

1. Dans le menu contextuel, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur `Serveur d'installation`, puis cliquez sur `Importer Serveur d'installation` pour lancer l'assistant. Reportez-vous à la figure 3-1 à la page 198.
3. Saisissez ou sélectionnez le nom du système que vous souhaitez importer. Cliquez sur `Terminer` pour importer le Serveur d'installation.

Importation d'un client compatible dans une cellule

Après avoir installé le logiciel Data Protector en local sur un client compatible cluster, importez le serveur virtuel représentant le client compatible cluster dans la cellule Data Protector.

Configuration système requise

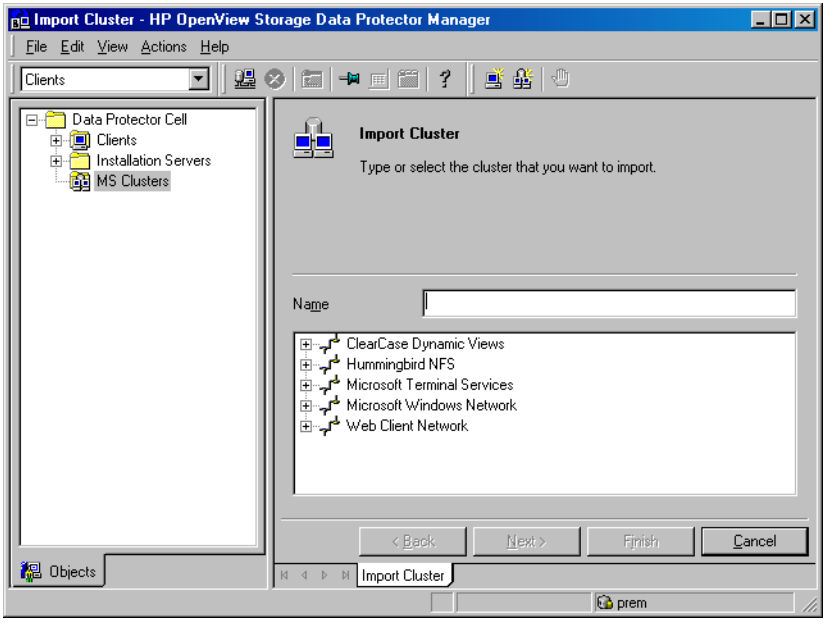
- Data Protector doit être installé sur tous les nœuds cluster.
- Tous les packages cluster doivent s'exécuter au sein du cluster.

Microsoft Cluster Server

Pour importer un client Microsoft Cluster Server dans la cellule Data Protector, procédez comme suit :

1. Dans le `Gestionnaire Data Protector`, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur `MS Clusters`, puis cliquez sur `Importer cluster`.
3. Saisissez le nom du serveur virtuel qui représente le client cluster à importer ou parcourez le réseau pour sélectionner le serveur virtuel. Consultez la figure 3-2.

Figure 3-2 **Importation d'un client Microsoft Cluster Server dans une cellule**



4. Cliquez sur `Terminer` pour importer le client cluster.

CONSEIL

Pour importer un nœud cluster ou un serveur virtuel spécifique, cliquez avec le bouton droit sur son cluster dans la fenêtre de navigation et cliquez sur `Importer noeud cluster` ou `Importer serveur virtuel cluster`.

Autres clusters

Configuration requise pour les clusters Tru64

Avant d'importer les noms d'hôtes de clusters, vérifiez les points suivants :

- Data Protector est installé sur le disque partagé dans le cluster.
- Tous les nœuds cluster Tru64 s'exécutent au sein du cluster.
- Le processus Data Protector `inetd` s'exécute sur chaque nœud.

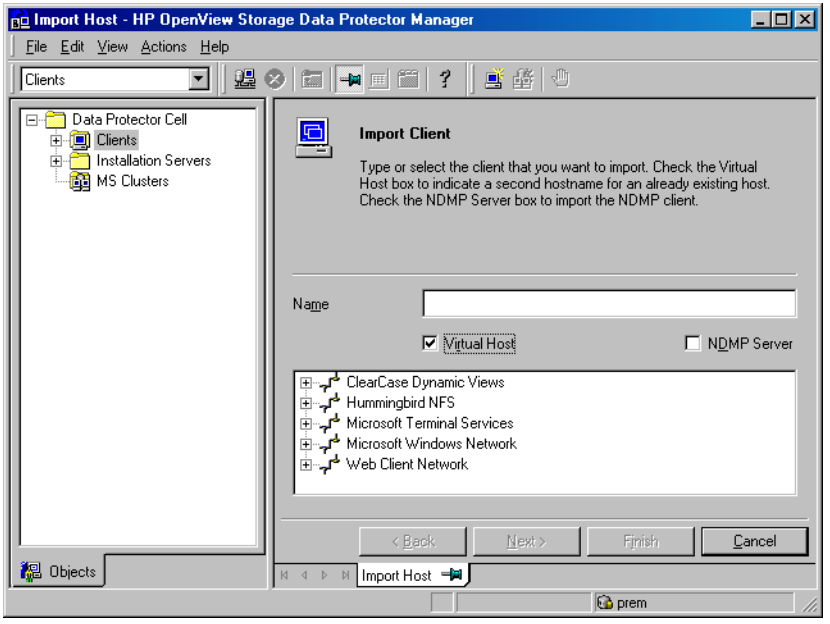
Procédure

Pour importer un client MC/ServiceGuard, Veritas, Tru64 Cluster ou Novell NetWare Cluster Services dans la cellule Data Protector, procédez comme suit :

1. Dans le `Gestionnaire Data Protector`, basculez vers le contexte `Clients`.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur `Clients`, puis cliquez sur `Importer clients`.
3. Saisissez le nom d'hôte du serveur virtuel tel qu'il est spécifié dans le package de clusters d'applications ou parcourez le réseau pour sélectionner le serveur virtuel (seulement si vous utilisez une interface graphique Windows) à importer.

   Sélectionnez l'option `Hôte virtuel` pour indiquer qu'il s'agit d'un serveur virtuel cluster. Consultez la figure 3-3.
4. Cliquez sur `Terminer` pour importer le serveur virtuel.

Figure 3-3 **Importation d'un client MC/ServiceGuard, Veritas ou Novell NetWare Cluster Services dans une cellule**



CONSEIL Pour configurer des sauvegardes de données sur les disques locaux des nœuds cluster, vous devez importer les nœuds cluster représentant les clients Data Protector. Pour connaître la procédure, reportez-vous à la section “Importation de clients dans une cellule” à la page 197.

Exportation de clients d'une cellule

L'exportation d'un client d'une cellule Data Protector revient à supprimer ses références de la base de données IDB sur le Gestionnaire de cellule sans pour autant désinstaller le logiciel du client. Cette procédure peut être réalisée à l'aide de l'interface graphique utilisateur Data Protector.

Vous pouvez avoir besoin de la fonction d'exportation dans les cas suivants :

- Vous souhaitez déplacer un client vers une autre cellule.
- Vous souhaitez supprimer un client des configurations de cellule Data Protector qui ne font plus partie du réseau.
- Vous souhaitez régler des problèmes dus à des licences insuffisantes.

  Lorsque vous exportez un client d'une cellule, la licence devient disponible pour un autre système.

Configuration système requise

Avant d'exporter un client, vérifiez les éléments suivants :

✓ Toutes les occurrences du client sont supprimées des spécifications de sauvegarde. Dans le cas contraire, Data Protector essaiera de sauvegarder des clients inconnus et cette partie de la spécification de sauvegarde échouera. Recherchez l'entrée suivante dans l'index de l'aide en ligne : "modification, spécification de sauvegarde" pour de plus amples informations sur la modification des spécifications de sauvegarde.

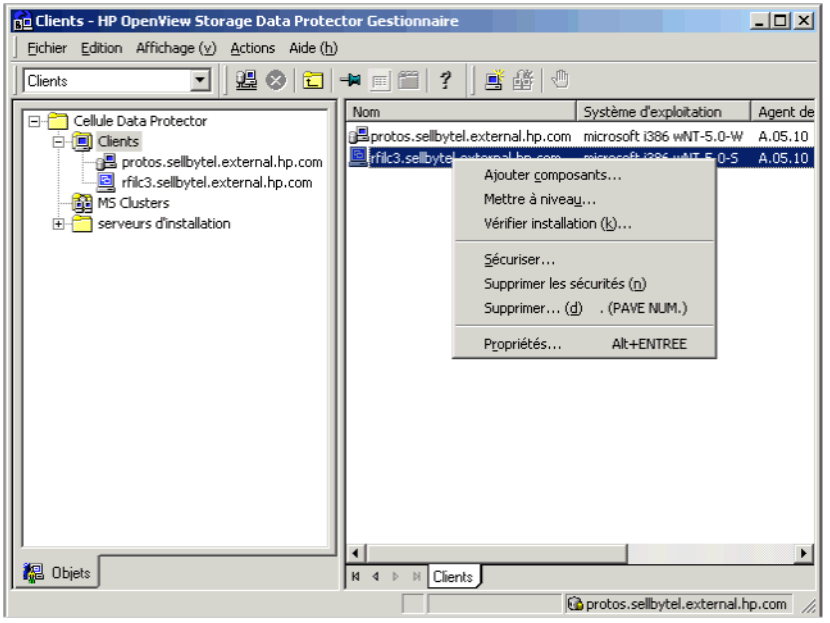
✓ Aucun périphérique de sauvegarde n'est connecté au client ni configuré sur ce dernier. Une fois le système exporté, Data Protector ne peut plus utiliser ses périphériques de sauvegarde dans la cellule d'origine.

Comment effectuer l'exportation ?

Afin d'exporter un client à l'aide de l'interface graphique utilisateur de Data Protector, procédez comme suit :

1. Dans le menu contextuel, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, cliquez sur `Clients`, cliquez avec le bouton droit de la souris sur le système client à exporter, puis cliquez sur `Supprimer`. Consultez la figure 3-4 à la page 205.

Figure 3-4 Exportation d'un système client



3. Un message vous demande si vous souhaitez également désinstaller le logiciel Data Protector. Cliquez sur `Non` pour exporter le client, puis sur `Terminer`.

Le client est supprimé de la liste dans la zone de résultats.

REMARQUE Vous ne pouvez pas exporter un client Data Protector avec le Serveur d'installation installé sur le même système que le client à exporter.

Clients Microsoft Cluster Server

Pour exporter un client Microsoft Cluster Server à partir de la cellule Data Protector, procédez comme suit :

1. Dans le menu contextuel, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, développez `MS Clusters`, cliquez avec le bouton droit de la souris sur le client cluster que vous souhaitez exporter, puis cliquez sur `Supprimer`.

3. Un message vous demande si vous souhaitez également désinstaller le logiciel Data Protector. Cliquez sur `Non` pour uniquement exporter le client cluster.

Le client cluster est supprimé de la liste dans la zone de résultats.

CONSEIL

Pour exporter un nœud cluster ou un serveur virtuel spécifique, cliquez avec le bouton droit de la souris sur le nœud cluster ou le serveur virtuel dans la fenêtre de navigation et cliquez sur `Supprimer`.

Considérations sur la sécurité

Cette section décrit les éléments de sécurité de Data Protector. Elle décrit les paramètres avancés pouvant être utilisés en vue d'améliorer la sécurité de Data Protector en tenant compte des connaissances préalables et des considérations requises.

L'amélioration de la sécurité dans un environnement complet étant assez complexe, de nombreuses fonctions de sécurité ne peuvent pas être activées par défaut.

Les considérations décrites dans ce chapitre s'appliquent non seulement lorsque des paramètres de sécurité sont modifiés, mais également lors de la configuration de nouveaux utilisateurs, de l'ajout de clients et de la configuration d'Agents d'application (ou toute autre modification à laquelle ces considérations s'appliquent). Toute modification apportée aux paramètres de sécurité peut avoir des répercussions dans la cellule toute entière et doit par conséquent être soigneusement planifiée.

Couches de sécurité

La sécurité doit être planifiée, testée et mise en oeuvre dans des couches de sécurité critique différentes afin d'assurer le fonctionnement sécurisé de Data Protector. Ces différentes couches correspondent aux clients Data Protector, aux Gestionnaire de cellule et aux utilisateurs. Cette section détaille la procédure de configuration de la sécurité sur chacune de ces couches.

Sécurité client

Les agents Data Protector installés sur les clients appartenant à la cellule offrent de nombreuses fonctionnalités puissantes, telles que l'accès à l'ensemble des données sur le système. Il est primordial que ces fonctionnalités ne soient disponibles que pour les processus s'exécutant sur les **autorités de cellule** (Gestionnaire de cellule et Serveur d’installation), et que toutes les autres requêtes soient refusées.

Avant de sécuriser les clients, il faut établir une liste d'hôtes fiables. Cette liste doit comprendre :

- Gestionnaire de cellule
- Serveurs d’installation concernés

- Pour certains clients, une liste de clients qui auront accès au robot à distance.

IMPORTANT

La liste doit contenir tous les noms d'hôte (ou adresses IP) possibles d'où les connexions peuvent provenir. Il est possible que plusieurs noms d'hôte soient nécessaires si l'un des clients mentionnés ci-dessus est multirésident (possède plusieurs cartes réseau et/ou plusieurs adresses IP) ou s'il s'agit d'un cluster.

Si la configuration DNS dans la cellule n'est pas uniforme, des considérations supplémentaires peuvent s'appliquer. Pour plus d'informations, reportez-vous à la section “Sécurisation des clients” à la page 210.

Même s'il peut ne pas être toujours indispensable de sécuriser chacun des clients contenus dans la cellule, il est important que les ordinateurs auxquels se fient d'autres clients soient eux-mêmes sécurisés :

- Gestionnaire de cellule / MoM
- Serveurs d’installation
- Clients Agent de support (MA)

REMARQUE

Les clients de l'interface utilisateur ne doivent pas être nécessairement ajoutés à la liste des clients fiables. En fonction des droits utilisateur, vous pouvez utiliser l'interface graphique utilisateur pour accéder à l'ensemble des fonctionnalités de Data Protector ou pour accéder seulement à des contextes spécifiques.

Utilisateurs de Data Protector

Pour procéder à la configuration des utilisateurs de Data Protector, vous devez tenir compte des aspects importants énumérés ci-dessous :

- Certains droits utilisateur accordent à l'utilisateur un grand pouvoir. Par exemple, les droits utilisateur `Configuration utilisateur` et `Configuration des clients` permettent à l'utilisateur de modifier les paramètres de sécurité. Le droit utilisateur `Restaurer vers autres clients` est également très puissant, en particulier (mais

pas exclusivement) s'il est associé à l'un des droits utilisateur suivants : `Sauvegarder en tant que root` ou `Restaurer en tant que root`.

- Même les droits utilisateur se caractérisant par un pouvoir moins important recèlent certains risques. Il est possible de configurer Data Protector en vue de restreindre certains droits utilisateur dans le but de réduire ces risques. Ces paramétrages sont décrits ultérieurement dans ce chapitre. Reportez-vous également à la section “Droit utilisateur de démarrage de spécification de sauvegarde” à la page 221.
- Data Protector est fourni seulement avec quelques groupes d'utilisateurs prédéfinis. Il est conseillé de définir des groupes spécifiques pour chaque type d'utilisateur dans l'environnement de Data Protector afin de limiter l'ensemble des droits qui leur sont octroyés.
- La configuration des utilisateurs dépend de la validation des utilisateurs (reportez-vous à la section “Vérification stricte du nom d'hôte” à la page 218). La validation renforcée peut s'avérer inutile en l'absence d'une configuration utilisateur détaillée et vice versa : la configuration utilisateur, aussi détaillée soit-elle, pourra être contournée si la validation renforcée n'est pas présente.
- Il est important que la liste des utilisateurs de Data Protector ne comporte pas de spécifications utilisateur "faibles". Notez que la partie `hôte` d'une spécification utilisateur constitue la partie éprouvée (en particulier avec la validation renforcée), alors que les parties `utilisateur` et `groupe` ne peuvent pas être vérifiées de manière fiable. Tout utilisateur doté de droits utilisateur puissants doit être configuré en particulier pour le client qu'il utilisera pour l'administration de Data Protector. S'il utilise plusieurs clients, une entrée doit être ajoutée pour chaque client supplémentaire. Evitez de spécifier l'utilisateur ainsi : `utilisateur`, `groupe`, `<Tout>`. L'accès à l'un de ces systèmes doit être interdit aux utilisateurs non fiables.

Dans l'index de l'aide en ligne, recherchez : “configuration, utilisateurs” pour plus d'informations sur la configuration des utilisateurs.

Sécurité du Gestionnaire de cellule

Il est essentiel de garantir la sécurité du Gestionnaire de cellule car ce dernier a accès à l'ensemble des clients et des données de la cellule.

La sécurité du Gestionnaire de cellule peut être renforcée via la fonctionnalité de vérification stricte de nom d'hôte. Il est toutefois important de sécuriser le Gestionnaire de cellule en tant que client et de configurer avec attention les utilisateurs de Data Protector. Reportez-vous aux sections “Vérification stricte du nom d'hôte” à la page 218 et “Sécurisation des clients” à la page 210.

Autres aspects de la sécurité

Vous devez également prendre en compte d'autres aspects liés à la sécurité :

- Les utilisateurs ne doivent pas avoir accès aux clients fiables (Gestionnaire de cellule, Serveur d’installation, MA et clients côté robotique). Même le fait d'autoriser une session `anonyme` ou un accès `ftp` peut présenter un risque sérieux pour l'ensemble de la sécurité.
- Les bibliothèques de supports et de bandes (et les clients qui y sont connectés) doivent être protégées physiquement contre l'accès de toute personne non autorisée ou non fiable.
- Pendant les opérations de sauvegarde, de restauration, de copie d'objets ou de supports, ou encore de consolidation d'objets, les données sont transférées via le réseau. Si la segmentation du réseau ne permet pas d'assurer une indépendance suffisante par rapport au réseau non sécurisé, il convient d'utiliser des périphériques connectés en local ou une bibliothèque de codage personnalisée. Notez qu'il est préférable d'effectuer une sauvegarde complète après la modification de la bibliothèque de codage.

Pour obtenir des informations sur les autres aspects liés à la sécurité, reportez-vous également au *Guide conceptuel HP OpenView Storage Data Protector*.

Sécurisation des clients

Après avoir installé les clients Data Protector et les avoir importés dans une cellule, il est vivement recommandé de les protéger afin d'empêcher l'accès de clients non autorisés.

Data Protector vous permet de spécifier les autorités de cellule (Gestionnaire de cellule, MoM et Serveur d’installation) dont un client acceptera les requêtes sur le port Data Protector `5555`. Ainsi, les autres ordinateurs ne seront pas en mesure d'accéder à ce client. Reportez-vous également à la section “Sécurité client” à la page 207.

REMARQUE Les clients qui auront accès au robot de bibliothèque doivent être ajoutés à la liste des autorités de cellule destinée aux clients du robot de bibliothèque.

Pour les activités telles que la restauration, la sauvegarde, le lancement pré-exécution ou post-exécution, l'importation et l'exportation de clients, le client vérifie si l'ordinateur qui déclenche l'une de ces tâches via le port Data Protector (port par défaut 5555), est autorisé à le faire. Ce mécanisme de sécurité donne l'instruction au client de n'accepter ce genre d'action que de la part des autorités de cellule spécifiées.

Situations exceptionnelles

Avant de commencer à restreindre l'accès aux clients, prenez en compte les cas suivants, qui peuvent poser des problèmes :

- Une autorité de cellule possède plusieurs cartes réseau et plusieurs adresses IP/noms de client.
- Le Gestionnaire de cellule est compatible cluster.
- Le robot d'une bibliothèque de bandes est configuré sur un système séparé (ou dédié).

Data Protector vous permet de définir toute une liste de systèmes explicitement autorisés à se connecter au client en tant qu'autorité de cellule. Afin d'éviter tout problème, préparez à l'avance la liste de tous les noms de client valides possibles pour d'autres autorités de cellule.

La liste doit contenir :

- Tous les noms de client supplémentaires (pour toutes les cartes réseau) de l'autorité de cellule.
- Les noms de client de tous les nœuds cluster sur lesquels le Gestionnaire de cellule risque de basculer, ainsi qu'un nom d'hôte de serveur virtuel cluster.
- Le nom du système cible vers lequel l'autorité de cellule sera déplacée en cas de panne matérielle totale de l'autorité de cellule. Ce système cible doit être défini dans la stratégie de récupération après sinistre.
- Pour les clients autorisés à accéder à un client commandant le robot d'une bibliothèque, tous les clients utilisant les lecteurs de cette dernière.

Le concept d'autorisation et de refus d'accès peut s'appliquer à l'ensemble des systèmes sur lesquels Data Protector est installé. Vous pouvez par exemple autoriser ou refuser l'accès d'un Gestionnaire de cellule à un client, d'un Gestionnaire de cellule à un Gestionnaire de cellule, d'un Serveur d'installation à un client ou d'un client à un client.

REMARQUE

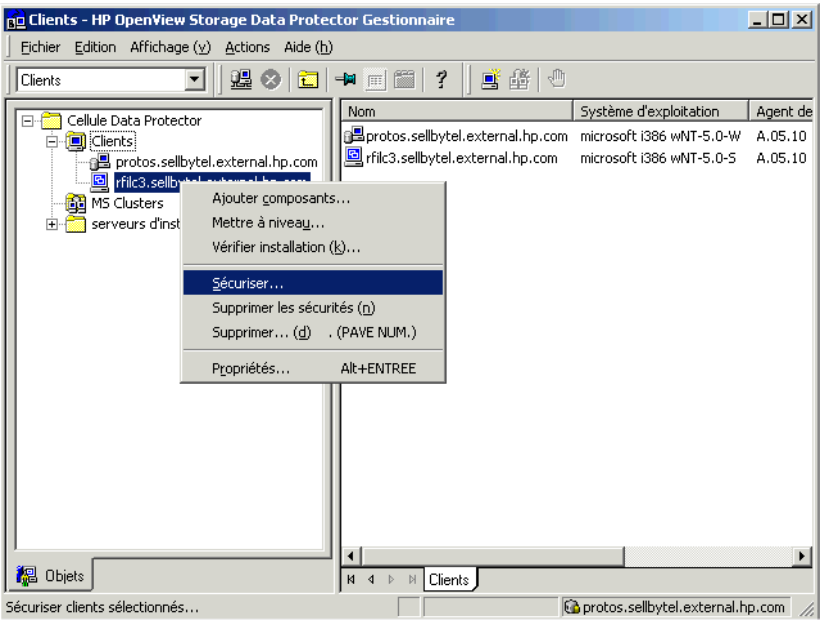
Si le Serveur d'installation résidant sur un système autre que le Gestionnaire de cellule n'est pas ajouté à la liste des clients autorisés, il n'a pas accès à un client sécurisé. Dans ce cas, les opérations dépendant du Serveur d'installation (vérification de l'installation, ajout de composants et suppression de clients, par exemple) échoueront. Si vous souhaitez que ces opérations soient disponibles sur le client sécurisé, ajoutez le Serveur d'installation à la liste des clients autorisés.

Procédure de sécurisation d'un client

Pour autoriser la vérification d'une autorité de cellule du côté client (sécuriser un client), effectuez les opérations suivantes dans l'interface graphique utilisateur de Data Protector :

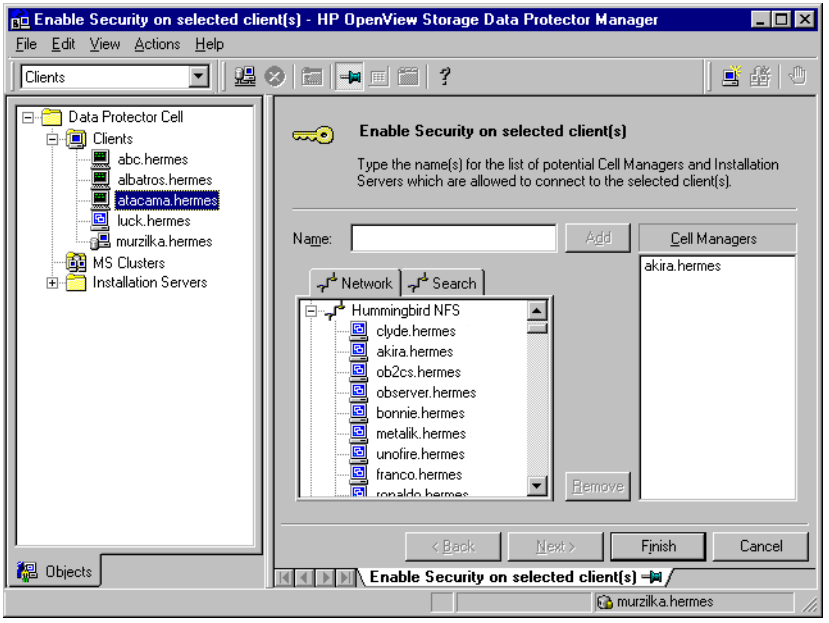
1. Dans le menu contextuel, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, développez `Clients`, cliquez avec le bouton droit de la souris sur le ou les clients que vous voulez sécuriser, puis cliquez sur `Sécuriser`. Consultez la figure 3-5.

Figure 3-5 Sécurisation d'un client



3. Saisissez les noms des systèmes qui auront accès aux clients sélectionnés ou recherchez ces systèmes en utilisant les onglets `Réseau` ou `Recherche`. Cliquez sur `Ajouter` pour ajouter chaque système à la liste. Consultez la figure 3-6.

Figure 3-6 Activation de la sécurité sur les clients sélectionnés



Le Gestionnaire de cellule reçoit automatiquement une autorisation d'accès et il est ajouté à la liste des clients fiables. Vous ne pouvez pas exclure le Gestionnaire de cellule de la liste.

4. Cliquez sur `Terminer` pour ajouter les systèmes sélectionnés au fichier `allow_hosts`.

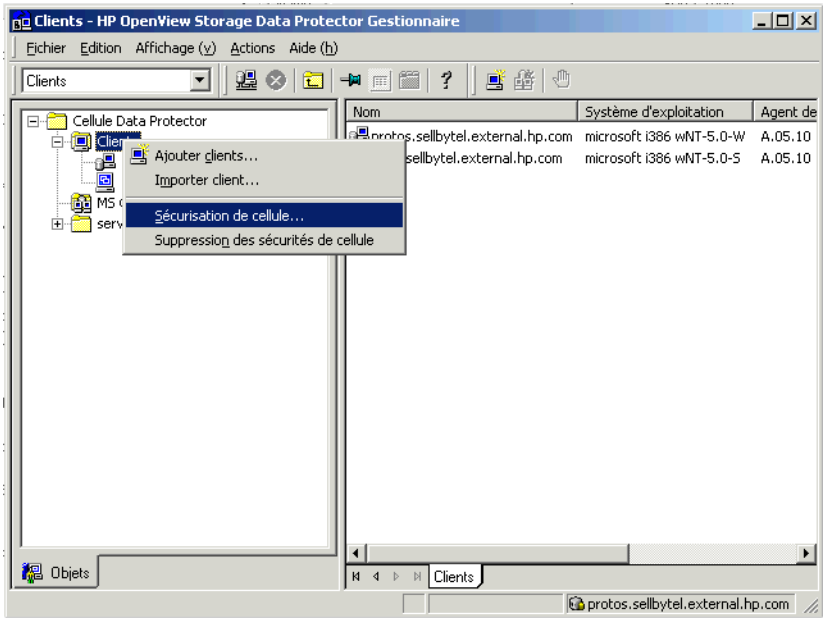
Que se passe-t-il ? Les clients vérifient la source de chaque requête provenant d'autres clients et n'autorisent que les requêtes reçues des clients sélectionnés dans la fenêtre `Activer la sécurité sur le(s) client(s) sélectionné(s)`. Ces clients sont répertoriés dans le fichier `allow_hosts`. Si une demande est refusée, l'événement est consigné dans le fichier `inet.log` dans le répertoire suivant :

- Sous Windows : *<répertoire_Data_Protector>*`\log`
- Sous HP-UX, Solaris et Linux : `/var/opt/omni/log`
- Sous les autres systèmes UNIX : `/usr/omni/log`

Pour sécuriser tous les clients de la cellule, procédez comme suit dans l'interface graphique de Data Protector :

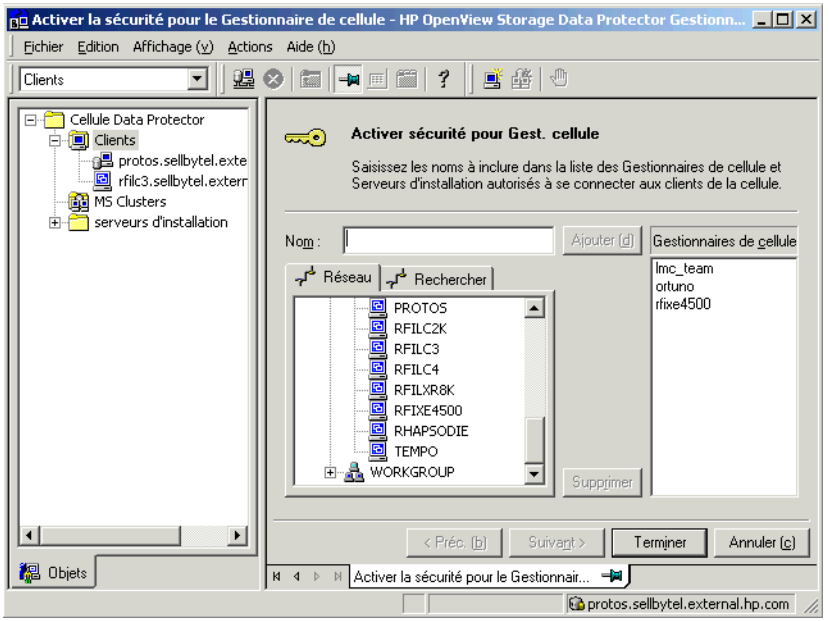
1. Dans le menu contextuel, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur `Clients`, puis cliquez sur `Sécurisation de cellule`. Consultez la figure 3-7.

Figure 3-7 Sécurisation d'une cellule



3. Saisissez les noms des systèmes qui auront accès à tous les clients dans la cellule ou recherchez ces systèmes en utilisant les onglets `Réseau` (seulement si vous utilisez une interface graphique Windows) ou `Recherche`. Cliquez sur `Ajouter` pour ajouter chaque système à la liste. Consultez la figure 3-8.

Figure 3-8 **Activation de la sécurité pour tous les clients de la cellule**



4. Cliquez sur `Terminer` pour ajouter les systèmes sélectionnés au fichier `allow_hosts`.

Que se passe-t-il ? Les clients vérifient la source de chaque requête provenant d'autres clients et n'autorisent que les requêtes reçues des clients sélectionnés dans la fenêtre `Activer la sécurité sur le Gestionnaire de cellule`. Ces clients sont répertoriés dans le fichier `allow_hosts`. Si une demande est refusée, l'événement est consigné dans le fichier `inet.log` dans le répertoire suivant :

- Sous Windows : *<répertoire_Data_Protector>*`\log`
- Sous HP-UX, Solaris et Linux : `/var/opt/omni/log`
- Sous les autres systèmes UNIX : `/usr/omni/log`

Lorsque vous sécurisez une cellule entière, tous les clients qui résident dans cette cellule sont sécurisés. Lorsque vous ajoutez un nouveau client à la cellule, sécurisez-le également.

Suppression de la sécurité

Pour supprimer la sécurité du ou des systèmes sélectionnés, procédez comme suit via l'interface graphique de Data Protector :

1. Dans le menu contextuel, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur le ou les clients pour lesquels vous voulez supprimer la sécurité, puis cliquez sur `Supprimer les sécurités`.
3. Cliquez sur `Oui` pour confirmer que vous autorisez l'accès aux clients sélectionnés.

Si vous voulez supprimer la sécurité de tous les clients présents dans la cellule, procédez comme suit :

1. Dans le menu contextuel, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur `Clients`, puis cliquez sur `Suppression des sécurités de cellule`.
3. Cliquez sur `Oui` pour confirmer que vous autorisez l'accès à tous les clients présents dans votre cellule.

Fichiers `allow_hosts` et `deny_hosts`

Lorsque vous sécurisez un client, les noms de client des systèmes autorisés à accéder à un client figurent dans le fichier `allow_hosts`. Vous pouvez aussi refuser explicitement l'accès à un client par certains ordinateurs en ajoutant leurs noms au fichier `deny_hosts`. Ces fichiers se trouvent dans le répertoire suivant :

- Sous Windows : *<répertoire_Data_Protector>*`\Config\client`
- Sous HP-UX, Solaris et Linux : `/etc/opt/omni/client`
- Sous les autres systèmes UNIX : `/usr/omni/config/client`

Indiquez un nom de client par ligne distincte.

REMARQUE

Si vous verrouillez un client par mégarde, vous pouvez modifier (ou supprimer) manuellement le fichier `allow_hosts` de ce client.

Sur les systèmes Windows, les fichiers sont au format codé sur deux octets (Unicode) ; sur les systèmes HP-UX, Solaris et Linux, en revanche, ils sont au format codé sur un octet ou sur plusieurs octets (Shift-JIS, par exemple).

Enregistrement excessif dans le fichier inet.log

Si les clients ne sont pas sécurisés et que le Gestionnaire de cellule est configuré dans l'environnement MC/ServiceGuard ou possède plusieurs noms ou numéros IP, le fichier `inet.log` peut contenir de nombreuses entrées du type suivant :

`Une requête 0 a été émise par l'hôte` *`nom.entreprise.com`* `qui n'est pas un Gestionnaire de cellule de ce client`

Ces entrées résultent du fait que le client, qui n'est pas sécurisé, ne reconnaît que le nom d'hôte principal du Gestionnaire de cellule. Les demandes provenant de tous les autres clients sont autorisées et enregistrées dans le fichier `inet.log`.

Lorsqu'un client est sécurisé, les demandes provenant des clients répertoriés dans le fichier `allow_hosts` sont acceptées et ne sont donc pas enregistrées. Les demandes provenant d'autres clients sont refusées.

La sécurisation des clients peut être une solution permettant d'éviter les entrées inutiles dans les fichiers `inet.log`. Néanmoins, il est préférable de répertorier tous les noms de client possibles pour le Gestionnaire de cellule dans le fichier `allow_hosts` de chaque client. L'accès au client est ainsi garanti, même en cas de basculement.

Si cette solution est impossible dans votre environnement pour une raison quelconque, vous pouvez sécuriser les clients et spécifier `*` comme plage d'adresses IP pour les systèmes auxquels vous souhaitez autoriser l'accès. Cela signifie que vos clients accepteront les requêtes provenant de tous les systèmes (n'importe quelle adresse IP) et ne seront pratiquement pas sécurisés, mais que vous pourrez néanmoins résoudre le problème des connexions excessives.

Vérification stricte du nom d'hôte

Par défaut, le Gestionnaire de cellule utilise une méthode relativement simple pour valider les utilisateurs. Il utilise le nom d'hôte tel qu'il est connu du client lorsqu'une interface utilisateur ou un agent d'application est démarré. Cette méthode est plus facile à configurer, offre un niveau

de sécurité convenable dans les environnements où la sécurité est considérée comme "conseillée" (c'est-à-dire où des attaques malveillantes ne se produisent normalement pas).

D'autre part, le paramètre de vérification stricte du nom d'hôte offre une validation renforcée des utilisateurs. Cette validation utilise le nom d'hôte tel qu'il est résolu par le Gestionnaire de cellule à l'aide de la recherche DNS inverse à partir de l'adresse IP obtenue par la connexion. Cela impose les limites et considérations suivantes :

Limites

- La validation des utilisateurs sur la base de l'adresse IP ne peut être qu'équivalente au niveau de protection contre l'usurpation d'adresse sur le réseau. Le concepteur du système de sécurité doit déterminer si le réseau en place offre un degré suffisant de protection contre l'usurpation d'adresse pour ces exigences de sécurité en particulier. La protection contre l'usurpation d'adresse peut être ajoutée en segmentant le réseau à l'aide de pare-feux, de routeurs, de VPN, etc.
- La séparation des utilisateurs au sein d'un client donné n'a pas un effet aussi important que la séparation des clients. Dans un environnement hautement sécurisé, il ne faut pas mélanger les utilisateurs courants et les utilisateurs dotés de droits importants au sein du même client.
- Les hôtes utilisés dans les spécifications utilisateur ne peuvent pas être configurés pour utiliser DHCP, sauf s'ils sont liés à une adresse IP fixe et configurés dans le DNS.

Soyez conscients des limites qui s'appliquent afin d'évaluer correctement le degré de sécurité pouvant être atteint avec la vérification stricte du nom d'hôte.

Résolution du nom d'hôte

Le nom d'hôte utilisé par Data Protector pour la validation peut varier entre la validation de l'utilisateur par défaut et la vérification stricte du nom d'hôte dans les situations suivantes :

- La recherche DNS inverse renvoie un nom d'hôte différent. Ce renvoi peut être volontaire ou peut révéler une mauvaise configuration du client ou de la table de DNS inverse.
- Le client est multirésident (possède plusieurs cartes réseau et/ou plusieurs adresses IP). L'application de cette considération à un client multirésident particulier dépend du rôle joué par ce dernier sur le réseau et de la manière dont il est configuré dans le DNS.
- Le client est un cluster.

En raison de la nature des vérifications pouvant être effectuées avec ce paramétrage, une reconfiguration des utilisateurs de Data Protector peut s'avérer nécessaire. Les spécifications existantes des utilisateurs de Data Protector doivent être vérifiées afin de savoir si elles peuvent être attribuées à l'une des raisons mentionnées ci-dessus. Selon le cas, les spécifications existantes devront éventuellement être modifiées ou de nouvelles spécifications ajoutées pour toutes les adresses IP possibles d'où peuvent provenir des connexions.

Notez que les utilisateurs doivent également être reconfigurés lorsque vous revenez à la validation de l'utilisateur par défaut, si vous avez dû modifier les spécifications de l'utilisateur lorsque vous avez activé la vérification stricte du nom d'hôte. Il est par conséquent recommandé de choisir une validation d'utilisateur et de la conserver.

Pour que la recherche DNS inverse soit fiable, le serveur DNS doit être sécurisé. Vous devez empêcher l'accès physique et la connexion à l'ensemble du personnel non autorisé.

En configurant des utilisateurs avec des adresses IP au lieu de noms d'hôte, vous pouvez éviter certains problèmes de validation liés au DNS ; toutefois, une telle configuration est plus difficile à gérer.

Conditions requises

La validation renforcée ne donne pas automatiquement accès à certaines connexions internes. Par conséquent, lorsque cette validation est utilisée, un nouvel utilisateur doit être ajouté pour chacun des éléments suivants :

- Un Agent d'application (OB2BAR) sur des clients Windows. Pour les clients Windows, il faut ajouter l'utilisateur `SYSTEM`, `NT AUTHORITY`, *`<client>`* pour chaque client disposant d'un Agent d'application installé. Remarquez que si `Inet` sur un client donné est configuré de manière à utiliser un compte spécifique, ce compte doit déjà avoir été paramétré. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "Vérification stricte du nom d'hôte".
- Si vous utilisez la fonctionnalité de génération de rapports Web, l'utilisateur `java`, `applet`, *`<nom_hôte>`* doit être ajouté pour chaque nom d'hôte à partir duquel la fonctionnalité de génération de rapports Web sera utilisée. Notez que pour bénéficier pleinement de la fonctionnalité de génération de rapports Web, les utilisateurs doivent appartenir au même groupe `admin`. Par conséquent, ces clients doivent être sécurisés. De même, avant de mettre à disposition des

autres utilisateurs des données ou la fonctionnalité de génération de rapports Web (par exemple, via un serveur Web), tenez compte des implications en matière de sécurité.

Pour obtenir des informations détaillées sur la configuration utilisateur, recherchez l'entrée suivante dans l'index de l'aide en ligne : "configuration, utilisateurs".

Activation de la fonction

Pour activer la vérification stricte du nom d'hôte, paramétrez l'indicateur `StrictSecurityFlags 0x0003` dans le fichier d'options globales.

Pour plus d'informations sur le fichier d'options globales, reportez-vous au *Guide de dépannage HP OpenView Storage Data Protector*.

Droit utilisateur de démarrage de spécification de sauvegarde

Pour obtenir des informations d'ordre général sur les utilisateurs de Data Protector et les droits utilisateur, recherchez l'entrée suivante dans l'index de l'aide en ligne : "utilisateurs".

Le droit utilisateur `Démarrage de spécification de sauvegarde` seul ne permet pas à un utilisateur d'utiliser le contexte de `sauvegarde` dans l'interface graphique utilisateur. L'utilisateur peut démarrer une spécification de sauvegarde à partir de la ligne de commande à l'aide de la commande `omnib` associée à l'option `-datalist` .

REMARQUE

S'il associe les droits utilisateur `Démarrer spécification de sauvegarde` et `Démarrer la sauvegarde`, un utilisateur peut visualiser les spécifications de sauvegarde configurées dans l'interface graphique utilisateur et il est en mesure de démarrer une spécification de sauvegarde ou une sauvegarde interactive.

Il n'est pas toujours souhaitable de permettre aux utilisateurs d'effectuer des sauvegardes interactives. Pour autoriser des sauvegardes interactives uniquement aux utilisateurs ayant le droit d'enregistrer une spécification de sauvegarde, paramétrez l'indicateur `StrictSecurityFlags 0x0200` dans le fichier d'options globales.

Pour plus d'informations sur le fichier d'options globales, reportez-vous au *Guide de dépannage HP OpenView Storage Data Protector*.

Masquage du contenu des spécifications de sauvegarde

Dans un environnement hautement sécurisé, le contenu des spécifications de sauvegarde enregistrées peut être considéré comme sensible, voire confidentiel. Il est possible de configurer Data Protector pour qu'il dissimule le contenu des spécifications de sauvegarde à tous les utilisateurs, à l'exception de ceux qui disposent des droits d'utilisateur `Enregistrer spécification de sauvegarde`. Pour ce faire, réglez l'indicateur `StrictSecurityFlags` sur `0x0400` dans le fichier d'options globales.

Pour plus d'informations sur le fichier d'options globales, reportez-vous au *Guide de dépannage HP OpenView Storage Data Protector*.

Groupement d'hôtes approuvés

La fonctionnalité de groupement d'hôtes approuvés réduit la nécessité d'accorder des droits d'utilisateur `Restaurer vers autres clients` lorsqu'ils doivent seulement restaurer les données d'un client à un autre parmi un nombre limité de clients. Vous pouvez définir des groupes d'hôtes qui échangeront des données en toute confiance.

Les groupements d'hôtes approuvés sont habituellement utilisés dans les situations suivantes :

- Pour les clients d'un même cluster (noeuds et serveur virtuel).
- Si le nom d'hôte d'un client est modifié et que les données des anciens objets sauvegarde doivent être restaurées.
- En cas d'incohérence entre le nom d'hôte du client et les objets sauvegarde en raison de problèmes liés au DNS.
- Si un utilisateur détient plusieurs clients et doit restaurer les données d'un client vers un autre.
- Lors de la migration de données d'un hôte vers un autre.

Configuration

Pour configurer les groupements d'hôtes approuvés, créez le fichier `/etc/opt/omni/server/cell/host_trusts` sur un Gestionnaire de cellule UNIX ou Linux ou créez le fichier *<répertoire_Data_Protector>*`\Config\Server\cell\host_trusts` sur un Gestionnaire de cellule Windows.

Les groupes d'hôtes qui se font confiance mutuellement sont définis en tant que listes de noms d'hôtes placées entre crochets. Par exemple :

Exemple

```
GROUP="cluster.domain.com"
{
    cluster.domain.com
    node1.domain.com
    node2.domain.com
}

GROUP="Bajo"
{
    computer.domain.com
    anothercomputer.domain.com
}
```

Surveillance des événements de sécurité

Si vous rencontrez un problème lors de l'utilisation de Data Protector, vous pouvez consulter les informations des fichiers journaux pour en trouver la cause. Par exemple, les événements consignés pourront vous aider à déterminer les utilisateurs ou clients incorrectement configurés.

Evénements de sécurité client

Les événements de sécurité client sont journalisés dans le fichier `inet.log` sur chaque client de la cellule :

- Sous Windows : *<répertoire_Data_Protector>*`\log`
- Sous HP-UX, Solaris ou Linux : `/var/opt/omni/log`
- Sous les autres systèmes UNIX : `/usr/omni/log`

Evénements de sécurité du Gestionnaire de cellule

Les événements de sécurité du Gestionnaire de cellule sont consignés dans le fichier `security.log` :

- Sur un Gestionnaire de cellule sous Windows : *<répertoire_Data_Protector>*`\log\server`
- Sur un Gestionnaire de cellule UNIX : `/var/opt/omni/server/log`

Contrôle des correctifs Data Protector installés

Vous pouvez vérifier quels correctifs Data Protector sont installés sur chaque système de la cellule.

Limites

Les limites relatives au contrôle des correctifs sont les suivantes :

- Le contrôle des correctifs ne peut être effectué que sur les clients Data Protector sur lesquels Data Protector A.05.10 ou ultérieur est installé. Si la commande détecte un client doté d'une version antérieure de Data Protector, un message d'erreur est renvoyé.
- Le contrôle des correctifs vérifie quels correctifs sont installés uniquement sur les membres de la même cellule.

Condition préalable

Pour utiliser cette fonctionnalité, le composant Interface utilisateur doit être installé.

REMARQUE

Si vous avez installé un correctif spécifique pour un site par le passé, celui-ci sera toujours répertorié dans le rapport des correctifs, même s'il a été par la suite inclus dans d'autres correctifs.

Pour vérifier quels sont les correctifs Data Protector installés sur un système donné dans une cellule, utilisez l'interface graphique utilisateur ou l'interface de ligne de commande Data Protector.

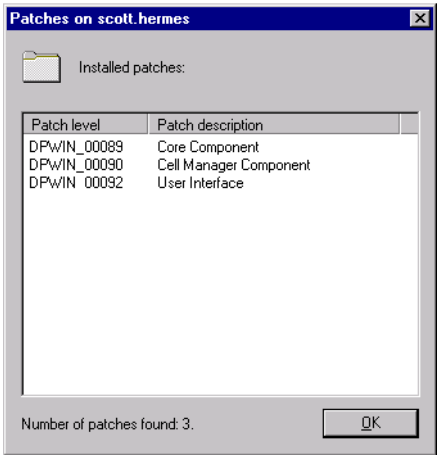
Contrôle des correctifs Data Protector à l'aide de l'interface graphique utilisateur

Pour vérifier quels sont les correctifs installés sur un client en particulier à l'aide de l'interface graphique utilisateur de Data Protector, procédez comme suit :

1. Dans le menu contextuel, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, développez `Clients` et sélectionnez un système de la cellule pour lequel vous souhaitez contrôler les correctifs installés.

3. Dans la zone de résultats, cliquez sur `Correctifs` pour ouvrir la fenêtre `Correctifs`.

Figure 3-9 Vérification des correctifs installés



Si des correctifs sont trouvés sur le système, la procédure de vérification retourne le niveau et la description de chaque chemin, ainsi que le nombre de correctifs installés.

S'il n'existe aucun correctif Data Protector sur le système, la procédure de vérification retourne une liste vide.

Si le système vérifié n'est pas un membre de la cellule, qu'il n'est pas disponible ou qu'une erreur se produit, la procédure de vérification retourne un message d'erreur.

4. Cliquez sur `OK` pour fermer la fenêtre.

Contrôle des correctifs Data Protector à l'aide de l'interface de ligne de commande

Pour vérifier quels sont les correctifs installés sur un client en particulier à l'aide de l'interface de ligne de commande Data Protector, exécutez la commande omnicheck -patches -host nom_hôte à partir du répertoire suivant :

- Sous Windows : `<répertoire_Data_Protector>\bin`
- Sous UNIX ou Linux : `/opt/omni/bin`

où *nom_hôte* est le nom du système à vérifier.

Pour en savoir plus sur la commande `omnicheck`, reportez-vous à la page `omnicheck` du manuel.

Désinstallation du logiciel Data Protector

Si la configuration de votre système change, vous souhaiterez peut-être désinstaller Data Protector du système ou retirer certains de ses composants logiciels.

La désinstallation consiste à supprimer tous les composants Data Protector du système, dont *toutes* les références à ce système provenant de la base de données IDB sur l'ordinateur du Gestionnaire de cellule. Cependant, les données de configuration de Data Protector restent sur le système par défaut pour que vous puissiez les utiliser pour la prochaine mise à niveau de Data Protector. Si vous souhaitez supprimer les données de configuration après la désinstallation du logiciel Data Protector, supprimez les répertoires dans lesquels Data Protector a été installé.

Si le répertoire dans lequel Data Protector est installé comporte d'autres données, vérifiez que vous les avez copiées dans un autre emplacement avant de procéder à la désinstallation de Data Protector. Dans le cas contraire, elles seront supprimées au moment de la désinstallation.

La désinstallation du logiciel Data Protector d'une cellule se déroule comme suit :

1. Désinstallation du logiciel client Data Protector à l'aide de l'interface graphique utilisateur. Reportez-vous à la section “Désinstallation d'un client Data Protector” à la page 229.
2. Désinstallation du Gestionnaire de cellule Data Protector et du Serveur d’installation. Reportez-vous à la section “Désinstallation du Gestionnaire de cellule et du Serveur d’installation” à la page 230.

Vous pouvez aussi désinstaller des composants logiciels de Data Protector sans désinstaller le Gestionnaire de cellule ou le client. Reportez-vous à la section “Changement de composants logiciels Data Protector” à la page 242.

Sous UNIX, vous pouvez également supprimer manuellement le logiciel Data Protector. Pour cela, reportez-vous à la section “Suppression manuelle du logiciel Data Protector sous UNIX” à la page 240.

Configuration système requise

Avant de désinstaller le logiciel Data Protector d'un ordinateur, vérifiez les points suivants :

✓ Vérifiez que toutes les références à l'ordinateur ont été supprimées des spécifications de sauvegarde. Dans le cas contraire, Data Protector essaiera de sauvegarder des systèmes inconnus et cette partie de la spécification de sauvegarde échouera. Recherchez l'entrée suivante dans l'index de l'aide en ligne : "modification, spécification de sauvegarde" pour de plus amples informations sur la modification des spécifications de sauvegarde.

✓ Vérifiez qu'aucun périphérique de sauvegarde n'est connecté ou configuré sur le système que vous voulez désinstaller. Une fois le système exporté, Data Protector ne peut plus utiliser ses périphériques de sauvegarde dans la cellule d'origine.

Désinstallation d'un client Data Protector

REMARQUE

La procédure de désinstallation à distance nécessite que le Serveur d'installation soit installé pour les plates-formes à partir desquelles vous désinstallez le logiciel de Data Protector.

Pour désinstaller un client à distance, procédez comme suit dans l'interface graphique de Data Protector :

1. Dans le menu contextuel, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, développez `Clients`, cliquez avec le bouton droit de la souris sur le client à désinstaller, puis cliquez sur `Supprimer`. Un message vous demande si vous souhaitez également désinstaller le logiciel Data Protector.
3. Cliquez sur `Oui` pour désinstaller tous les composants logiciels du client, puis sur `Terminer`.

Le client sera supprimé de la liste figurant dans la zone de résultats et le logiciel Data Protector sera supprimé de son disque dur.

Notez que les données de configuration de Data Protector restent sur le système client. Si vous souhaitez supprimer les données de configuration, supprimez les répertoires dans lesquels Data Protector a été installé.

Clients cluster

Si votre environnement Data Protector comprend des clients compatibles cluster dans et que vous souhaitez les désinstaller, vous devez le faire localement. La procédure est la même que pour la désinstallation du Gestionnaire de cellule ou du Serveur d'installation. Reportez-vous à la section “Désinstallation du Gestionnaire de cellule et du Serveur d'installation” à la page 230.

Le client cluster sera supprimé de la liste figurant dans la zone de résultats et le logiciel Data Protector sera supprimé de son disque dur.

TruCluster

Pour désinstaller des clients TruCluster, exportez d'abord le noeud virtuel. Désinstallez ensuite les clients Data Protector du ou des noeuds.

Clients OpenVMS

Un client OpenVMS Data Protector ne peut pas être supprimé à distance avec un Serveur d'installation. Il doit être désinstallé localement.

Pour désinstaller un client Data Protector d'un système OpenVMS, procédez comme suit :

1. Commencez par exporter le client concerné à partir de la cellule Data Protector dans l'interface graphique de ce dernier, comme l'indique la section “Exportation de clients d'une cellule” à la page 204.

   A la question demandant si vous souhaitez désinstaller également le logiciel Data Protector, répondez `Non`.

2. Pour supprimer réellement le logiciel client Data Protector, connectez-vous au compte `SYSTEM` du client OpenVMS et exécutez la commande suivante :
   `$ PRODUCT REMOVE DP`
   A l'invite, répondez `OUI`.

IMPORTANT

Cette action ferme le service Data Protector et supprime tous les répertoires, fichiers et comptes associés à Data Protector sur le système OpenVMS.

Désinstallation du Gestionnaire de cellule et du Serveur d'installation

Cette section décrit la procédure permettant de désinstaller le Gestionnaire de cellule et le Serveur d'installation Data Protector des systèmes Windows, HP-UX et Solaris.

Désinstallation dans un système Windows

Désinstallation sur un système MS Cluster Server

Si vous avez installé l'utilitaire HP OpenView AutoPass en même temps que Data Protector sur un nœud Microsoft Cluster Server, vous devez désinstaller Data Protector de ce même nœud ; dans le cas contraire, AutoPass *ne* sera *pas* désinstallé.

Pour désinstaller le logiciel Data Protector d'un système Windows, procédez comme suit :

1. Assurez-vous que toutes les sessions de Data Protector sont terminées et que vous avez quitté l'interface graphique utilisateur.
2. Dans le Panneau de configuration de Windows, cliquez sur `Ajout/Suppression de programmes`.
3. Selon que vous ayez installé HP OpenView AutoPass ou non et selon que vous souhaitiez supprimer les données de configuration de Data Protector ou non, différentes actions sont possibles.

IMPORTANT

Si vous laissez les données de configuration de Data Protector sur le système après la désinstallation et que vous réinstallez plus tard une version antérieure du Gestionnaire de cellule Data Protector à celle qui était installée, notez que les données de configuration ne seront pas compatibles.

Pour installer correctement une version antérieure, lors de l'installation, choisissez l'option qui supprime les données de configuration.

Pour ce faire, procédez comme suit :

- Si l'utilitaire AutoPass a été installé avec Data Protector :

  Sélectionnez `HP OpenView Storage Data Protector A.06.00` et cliquez sur `Changer` puis sur `Suivant`. Dans la boîte de dialogue Maintenance du programme, cliquez sur `Supprimer`. Pour supprimer définitivement les données de configuration de Data Protector, sélectionnez `Supprimer définitivement les données de configuration`. Dans le cas contraire, cliquez sur `Suivant`.

Si AutoPass a été installé en même temps que Data Protector et que Data Protector est la seule application qui l'utilise, AutoPass est supprimé. Dans le cas contraire, seul l'enregistrement d'AutoPass auprès de Data Protector est annulé, mais l'utilitaire reste installé.

- Si AutoPass n'a pas été installé :
  - Pour désinstaller Data Protector et conserver les données de configuration Data Protector sur le système, sélectionnez `HP OpenView Storage Data Protector A.06.00` et cliquez sur `Supprimer`.
  - Pour désinstaller Data Protector et supprimer les données de configuration Data Protector, sélectionnez `HP OpenView Storage Data Protector A.06.00`, cliquez sur `Changer` puis sur `Suivant`. Dans la boîte de dialogue Maintenance du programme, cliquez sur `Supprimer`. Sélectionnez `Supprimer définitivement les données de configuration` et cliquez sur `Suivant`.

4. Lorsque la désinstallation est terminée, cliquez sur `Terminer` pour quitter l'assistant.

   Si AutoPass est supprimé au cours de la désinstallation du Gestionnaire de cellule, appuyez sur **F5**dans la fenêtre `Ajout/Suppression de programmes` pour réactualiser la liste des programmes et composants installés.

Désinstallation dans un système HP-UX

IMPORTANT

Si vous laissez les données de configuration de Data Protector sur le système après la désinstallation et que vous réinstallez plus tard une version antérieure du Gestionnaire de cellule Data Protector à celle qui était installée, notez que les données de configuration ne seront pas compatibles.

Pour installer correctement une version antérieure, après la désinstallation, supprimez les répertoires Data Protector de votre système.

Avant de commencer à désinstaller le logiciel Data Protector, arrêtez tous les processus Data Protector en cours d'exécution sur le système du Gestionnaire de cellule et/ou du Serveur d'installation :

1. Connectez-vous en tant que `root` et exécutez la commande `omnisv -stop` à partir du répertoire `/opt/omni/sbin`.
2. Tapez la commande `ps -ef | grep omni` pour vérifier si tous les processus ont bien été arrêtés. Aucun processus Data Protector ne devrait être répertorié sur exécution de la commande `ps -ef | grep omni`.

   Si vous avez des processus Data Protector en cours d'exécution, arrêtez-les à l'aide de la commande `kill -9 <ID_processus>` avant de procéder à la désinstallation.
3. Exécutez `/usr/sbin/swremove DATA-PROTECTOR` pour désinstaller le logiciel Data Protector.
4. L'utilitaire HP OpenView AutoPass n'est pas supprimé lors de la désinstallation de Data Protector. Vous pouvez le supprimer manuellement en exécutant la commande `/usr/sbin/swremove HPOVLIC` en tant qu'utilisateur root.

Pour supprimer les répertoires restants de Data Protector de votre système, reportez-vous à la section “Suppression manuelle du logiciel Data Protector sous UNIX” à la page 240.

Désinstallation du Gestionnaire de cellule et/ou du Serveur d'installation configuré(s) sur MC/ServiceGuard

Si votre Gestionnaire de cellule et/ou votre Serveur d'installation sont configurés sur un cluster MC/ServiceGuard, procédez comme suit pour désinstaller le logiciel.

Nœud principal

Connectez-vous au nœud principal et procédez comme suit :

1. Arrêtez le package Data Protector :

   `cmhaltpkg <nom_pkg>`

   où *<nom_pkg>* correspond au nom du package de clusters.

   Par exemple :

   `cmhaltpkg ob2cl`

2. Désactivez le mode cluster pour le groupe de volumes :

   ```
   vgchange -c n <nom_gv>
   ```

   (où *<nom_gv>* correspond au nom du chemin du groupe de volumes placé dans le sous-répertoire du répertoire `/dev`).

   Par exemple :

   ```
   vgchange -c n /dev/vg_ob2cm
   ```

3. Activez le groupe de volumes :

   ```
   vgchange -a y -q y <nom_gv>
   ```

   Par exemple :

   ```
   vgchange -a y -q y /dev/vg_ob2cm
   ```

4. Montez le volume logique sur le disque partagé :

   ```
   mount <chemin_vl> <disque_partagé>
   ```

   (où *<chemin_vl>* correspond au nom de chemin du volume logique et où *<disque_partagé>* correspond au point de montage ou répertoire partagé).

   Par exemple :

   ```
   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
   ```

5. Supprimez Data Protector à l'aide de l'outil `swremove`.
6. Supprimez les liens programmables :

   ```
   rm /etc/opt/omni
   ```

   ```
   rm /var/opt/omni
   ```

7. Supprimez les répertoires de sauvegarde :

   ```
   rm -rf /etc/opt/omni.save
   ```

   ```
   rm -rf /var/opt/omni.save
   ```

8. Supprimez le répertoire Data Protector et son contenu :

   ```
   rm -rf /opt/omni
   ```

9. Vous pouvez supprimer l'utilitaire HP OpenView AutoPass en exécutant la commande `/usr/sbin/swremove HPOVLIC` en tant qu'utilisateur root.

10. Démontez le disque partagé :

    umount *<disque_partagé>*

    Par exemple :

    umount /omni_shared

11. Désactivez le groupe de volumes :

    vgchange -a n *<nom_gv>*

    Par exemple :

    vgchange -a n /dev/vg_ob2cm

Nœud secondaire

Connectez-vous au nœud secondaire et procédez comme suit :

1. Activez le groupe de volumes :

   vgchange -a y *<nom_gv>*

2. Montez le disque partagé :

   mount *<chemin_vl>* *<disque_partagé>*

3. Supprimez Data Protector à l'aide de l'outil `swremove`.
4. Supprimez les liens programmables :

   rm /etc/opt/omni

   rm /var/opt/omni

5. Supprimez les répertoires de sauvegarde :

   rm -rf /etc/opt/omni.save

   rm -rf /var/opt/omni.save

6. Supprimez le répertoire Data Protector et son contenu :

   rm -rf /opt/omni

7. Supprimez les répertoires du système de fichiers partagé :

   rm -rf *<disque_partagé>*/etc_opt_omni

   rm -rf *<disque_partagé>*/var_opt_omni

   Par exemple :

   rm -rf /omni_shared/etc_opt_omni

   rm -rf /omni_shared/etc_opt_omni

8. Vous pouvez supprimer l'utilitaire HP OpenView AutoPass en exécutant la commande `/usr/sbin/swremove HPOVLIC` en tant qu'utilisateur root.
9. Démontez le disque partagé :

   `umount <disque_partagé>`
10. Désactivez le groupe de volumes :

    `vgchange -a n <nom_gv>`

Data Protector est complètement supprimé du système.

Désinstallation dans les systèmes Solaris

Gestionnaire de cellule

Le Gestionnaire de cellule pour Solaris est toujours installé en local, à l'aide de la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé en local à l'aide de l'utilitaire `pkgrm`.

IMPORTANT

Si vous laissez les données de configuration de Data Protector sur le système après la désinstallation et que vous réinstallez plus tard une version antérieure du Gestionnaire de cellule Data Protector à celle qui était installée, notez que les données de configuration ne seront pas compatibles.

Pour installer correctement une version antérieure, après la désinstallation, supprimez les répertoires Data Protector de votre système.

Pour désinstaller le Gestionnaire de cellule Data Protector, procédez comme suit :

1. Assurez-vous que vous avez terminé toutes les sessions de Data Protector et quitté l'interface graphique utilisateur.
2. Entrez la commande `pkginfo | grep OB2` pour répertorier tous les packages Data Protector installés sur le Gestionnaire de cellule.

   Les packages associés au Gestionnaire de cellule se répartissent comme suit :

OB2-CORE	Logiciel central Data Protector
OB2-C-IS	Logiciel du Serveur d'installation

OB2-CS	Logiciel du Gestionnaire de cellule
OB2-CC	Logiciel de la console de cellule, contenant l'interface graphique utilisateur et l'interface de ligne de commande

Si des clients Data Protector ou Serveur d'installation sont aussi installés sur le système, les autres packages seront également répertoriés.

REMARQUE Si vous souhaitez laisser tout autre composant Data Protector installé, vous devez conserver le package OB2-CORE car il est indispensable au fonctionnement des autres packages.

3. Supprimez dans l'ordre inverse de celui où il ont été installés les packages mentionnés dans l'étape précédente par la commande `pkgrm <nom du package>` et suivez les instructions qui apparaissent sur la ligne de commande.
4. L'utilitaire HP OpenView AutoPass n'est pas supprimé lors de la désinstallation de Data Protector. Vous pouvez le supprimer manuellement en exécutant les commandes suivantes en tant qu'utilisateur root :

```
swremove HPOvLic
swremove HPOvLicJ
```

Serveur d'installation

Le Serveur d'installation pour UNIX sur Solaris est toujours installé en local à l'aide de la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé en local à l'aide de l'utilitaire `pkgrm`.

Pour désinstaller le Serveur d'installation Data Protector, procédez comme suit :

1. Assurez-vous que toutes les sessions de Data Protector sont terminées et que vous avez quitté l'interface graphique utilisateur.
2. Entrez la commande `pkginfo | grep OB2` pour répertorier tous les packages Data Protector installés sur le système du Serveur d'installation.

Les packages associés au Serveur d'installation se répartissent comme suit :

OB2-CORE	Logiciel central Data Protector
OB2-C-IS	Logiciel central Serveur d'installation
OB2-SOLUX	Ensembles de l'Agent de disque, de l'Agent de support et de l'interface graphique utilisateur pour les systèmes Solaris distants
OB2-OTHUX	Ensembles de l'Agent de disque et de l'Agent de support pour systèmes UNIX non-Solaris distants

Si d'autres composants Data Protector sont installés sur le système, ils seront également répertoriés.

REMARQUE Si vous souhaitez laisser tout autre composant Data Protector installé, vous devez conserver le package OB2-CORE car il est indispensable au fonctionnement des autres packages.

3. Supprimez dans l'ordre inverse de celui où il ont été installés les packages mentionnés dans l'étape précédente par la commande `pkgrm <nom du package>` et suivez les instructions qui apparaissent sur la ligne de commande.

Désinstallation dans les systèmes Linux

Gestionnaire de cellule Le Gestionnaire de cellule pour Linux est toujours installé en local, à l'aide de la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé en local à l'aide de l'utilitaire `rpm`.

IMPORTANT Si vous laissez les données de configuration de Data Protector sur le système après la désinstallation et que vous réinstallez plus tard une version antérieure du Gestionnaire de cellule Data Protector à celle qui était installée, notez que les données de configuration ne seront pas compatibles.

Pour installer correctement une version antérieure, après la désinstallation, supprimez les répertoires Data Protector de votre système.

Pour désinstaller le Gestionnaire de cellule Data Protector, procédez comme suit :

1. Assurez-vous que vous avez terminé toutes les sessions de Data Protector et quitté l'interface graphique utilisateur.
2. Entrez la commande `rpm -qa | grep OB2` pour répertorier tous les packages Data Protector installés sur le Gestionnaire de cellule.

   Les packages associés au Gestionnaire de cellule se répartissent comme suit :

OB2-CORE	Logiciel central Data Protector
OB2-CORE-IS	Logiciel du Serveur d'installation
OB2-CS	Logiciel du Gestionnaire de cellule
OB2-CC	Logiciel de la console de cellule, contenant l'interface de ligne de commande

   Si des clients Data Protector ou Serveur d'installation sont aussi installés sur le système, les autres packages seront également répertoriés.

REMARQUE Si vous souhaitez laisser tout autre composant Data Protector installé, vous devez conserver le package OB2-CORE car il est indispensable au fonctionnement des autres packages.

3. Supprimez dans l'ordre inverse de celui où ils ont été installés les packages mentionnés dans l'étape précédente par la commande `rpm -e<nom du package>` et suivez les instructions qui apparaissent sur la ligne de commande.

Serveur d'installation

Le Serveur d'installation pour UNIX sous Linux est toujours installé en local à l'aide de la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé en local à l'aide de l'utilitaire `rpm`.

Pour désinstaller le Serveur d'installation Data Protector, procédez comme suit :

1. Assurez-vous que toutes les sessions de Data Protector sont terminées et que vous avez quitté l'interface graphique utilisateur.

2. Entrez la commande `rpm -qa | grep OB2` pour répertorier tous les packages Data Protector installés sur le Serveur d'installation.

   Les packages associés au Serveur d'installation se répartissent comme suit :

OB2-CORE	Logiciel central Data Protector
OB2-CORE-IS	Logiciel central Serveur d'installation
OB2-LINUXP	Ensembles de l'Agent de disque, de l'Agent de support et de l'interface graphique utilisateur pour les systèmes Linux distants
OB2-OTHUXP	Ensembles de l'Agent de disque et de l'Agent de support pour systèmes UNIX non-Linux distants

   Si d'autres composants Data Protector sont installés sur le système, ils seront également répertoriés.

REMARQUE Si vous souhaitez laisser tout autre composant Data Protector installé, vous devez conserver le package OB2-CORE car il est indispensable au fonctionnement des autres packages.

3. Supprimez dans l'ordre inverse de celui où il ont été installés les packages mentionnés dans l'étape précédente par la commande `rpm -e <nom du package>` et suivez les instructions qui apparaissent sur la ligne de commande.

Suppression manuelle du logiciel Data Protector sous UNIX

Avant de désinstaller un client UNIX, vous devez l'exporter de la cellule. Pour connaître la procédure, reportez-vous à la section “Exportation de clients d'une cellule” à la page 204.

Systèmes HP-UX Pour supprimer manuellement les fichiers d'un système HP-UX, procédez comme suit :

1. Exécutez `/usr/sbin/swremove DATA-PROTECTOR` pour supprimer le logiciel Data Protector.

2. Supprimez les répertoires suivants à l'aide de la commande `rm` :

   ```
   rm -fr /var/opt/omni
   rm -fr /etc/opt/omni
   rm -fr /opt/omni
   ```

   A ce stade, les références Data Protector ne figurent plus sur votre système.

Systèmes Solaris

Pour supprimer manuellement les fichiers d'un système Solaris, supprimez-les des répertoires suivants, puis supprimez les répertoires à l'aide de la commande `rm` :

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
rm -fr /opt/omni
```

Systèmes Linux

Pour supprimer manuellement les fichiers d'un système Linux, supprimez-les des répertoires suivants, puis supprimez les répertoires à l'aide de la commande `rm` :

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
rm -fr /opt/omni
```

Autres systèmes UNIX

Supprimez les fichiers du répertoire suivant, puis supprimez le répertoire à l'aide de la commande `rm` :

```
rm -fr /usr/omni
```

Changement de composants logiciels Data Protector

Cette section décrit la procédure de suppression et d'ajout de composants logiciels Data Protector sur les systèmes Windows, HP-UX et Solaris. Pour obtenir la liste des composants Data Protector pris en charge selon les systèmes d'exploitation, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

Les composants logiciels Data Protector peuvent être ajoutés sur le Gestionnaire de cellule ou sur un client à l'aide de l'interface graphique utilisateur de Data Protector. L'installation à distance de composants sélectionnés s'effectue à l'aide de la fonctionnalité Serveur d'installation. Pour en connaître la procédure détaillée, reportez-vous à la section “Installation distante de clients Data Protector” à la page 54.

Les composants Data Protector peuvent être supprimés en local sur le Gestionnaire de cellule ou sur un client.

Sur les systèmes Windows

Pour ajouter ou supprimer des composants logiciels Data Protector sous Windows, procédez comme suit :

1. Dans le Panneau de configuration de Windows, cliquez sur `Ajout/Suppression de programmes`.
2. Sélectionnez `HP OpenView Storage Data Protector A.06.00` et cliquez sur `Modifier`.
3. Cliquez sur `Suivant`.
4. Dans la fenêtre `Maintenance du programme`, cliquez sur `Modifier`, puis sur `Suivant`.
5. Dans la fenêtre `Installation personnalisée`, sélectionnez les composants à ajouter et/ou désélectionnez les composants à supprimer. Cliquez sur `Suivant`.
6. Cliquez sur `Installer` pour lancer l'installation ou la suppression des composants logiciels.
7. Lorsque l'installation est terminée, cliquez sur `Terminer`.

Clients compatibles cluster

Si vous modifiez les composants logiciels de Data Protector sur les clients compatibles cluster, vous devez le faire localement, à partir du DVD-ROM, sur chaque nœud de cluster. Ensuite, vous devez importer manuellement le nom d'hôte du serveur virtuel dans la cellule Data Protector à l'aide de l'interface utilisateur.

Sur les systèmes HP-UX

Vous pouvez ajouter de nouveaux composants à l'aide de la fonctionnalité Serveur d'installation. Sur les systèmes HP-UX, certains composants Data Protector dépendent les uns des autres et ne pourront fonctionner correctement si vous supprimez l'un d'entre eux.

Le tableau ci-dessous présente les composants et leurs interdépendances :

Tableau 3-1 Dépendances de composants logiciels Data Protector sous HP-UX

Composants	dépendent de...
OMNI-MOMGUI	OMNI-CC
OMNI-CC, OMNI-CORE-IS	OMNI-CORE
OMNI-CS	OMNI-CORE, OMNI-CC
OMNI-INTEG, OMNI-DA, OMNI-MA ou OMNI-NDMP	OMNI-CORE
OMNI-NDMP-P	OMNI-CORE-IS
OMNI-INF-P, OMNI-SYB-P, OMNI-ORA-P, OMNI-OR8-P, OMNI-SAP-P, OMNI-SAPDB-P, OMNI-DB2-P, OMNI-EMC-P, OMNI-SSEA-P, OMNI-SNAPA-P, OMNI-SMISA-P	OMNI-INTEG OMNI-CORE-IS
OMNI-HPUX-P, OMNI-OTHUX-P, OMNI-OMNIST	OMNI-CORE-IS
OMNI-LOTUS-P, OMNI-OV-P	OMNI-CORE-IS

Procédure

Pour supprimer des composants logiciels Data Protector, procédez comme suit :

1. Connectez-vous en tant que `root`, puis exécutez la commande `swremove`.

2. Cliquez deux fois sur `B6960MA`, `DATA-PROTECTOR`, puis sur `OB2-CM` pour afficher une liste des composants Data Protector.
3. Sélectionnez les composants à supprimer.
4. Dans le menu `Actions`, cliquez sur `Marquer pour suppression` pour repérer les composants devant être supprimés.
5. Après avoir marqué les composants à supprimer, cliquez sur `Supprimer` dans le menu `Actions`, puis sur `OK`.

REMARQUE

Lorsque vous marquez les composants Data Protector à supprimer et que la suppression de ceux-ci risque d'affecter le fonctionnement d'autres composants, la boîte `Dépendances` apparaît pour vous présenter la liste des composants dépendants.

Spécificités d'Oracle

Après la désinstallation de l'intégration Oracle Data Protector sur un système de serveur Oracle, le logiciel Oracle Server reste lié à la bibliothèque de base de données Data Protector. Vous devez supprimer ce lien, faute de quoi vous ne pourrez pas démarrer le serveur Oracle après suppression de l'intégration. Reportez-vous à la section “Utilisation d'Oracle après le retrait de l'intégration d'Oracle dans Data Protector” dans le *Guide d’intégration HP OpenView Storage Data Protector*.

Sur les systèmes Solaris

Vous pouvez ajouter de nouveaux composants à l'aide de la fonctionnalité Serveur d’installation. Sur les systèmes Solaris, certains composants logiciels Data Protector dépendent les uns des autres et ne pourront fonctionner correctement si vous supprimez l'un d'entre eux.

Le tableau ci-dessous présente les composants et leurs interdépendances :

Tableau 3-2 Dépendances des composants logiciels Data Protector sous Solaris

Composants	dépendent de...
OB2-MOMGUI	OB2-CC
OB2-CC, OB2-C-IS	OB2-CORE
OB2-CS	OB2-CORE, OB2-CC

Tableau 3-2 Dépendances des composants logiciels Data Protector sous Solaris

Composants	dépendent de...
OB2-INTGP, OB2-DA, OB2-MA ou OB2-NDMPP	OB2-CORE
OB2-SOLUX	OB2-C-IS
OB2-INFP, OB2-SYBP, OB2-OR8P, OB2-SAPP, OB2-SAPDP, OB2-DB2P, OB2-SSEAP, OB2-SMISP	OB2-INTGP OB2-C-IS
OB2-OTHUX, OB2-OSTP, OB2-LOTP, OB2-OVP	OB2-C-IS

Procédure

Pour supprimer des composants logiciels Data Protector sur des systèmes Solaris, procédez comme suit :

1. Assurez-vous que toutes les sessions de Data Protector sont terminées et que vous avez quitté l'interface graphique utilisateur.
2. Entrez la commande `pkginfo | grep OB2` pour répertorier tous les packages Data Protector installés.
3. Supprimez dans l'ordre inverse de celui où il ont été installés les packages mentionnés dans l'étape précédente par la commande `pkgrm <nom du package>` et suivez les instructions qui apparaissent sur la ligne de commande.

Autres systèmes UNIX

Lorsque vous supprimez manuellement des composants d'un client Data Protector sur un système UNIX autre que Solaris ou HP-UX, mettez à jour le fichier `omni_info` dans le répertoire `/usr/omni/bin/install/omni_info`.

Pour chacun des composants désinstallés, supprimez la chaîne de version du composant associé dans le fichier `omni_info`.

Si vous supprimez simplement des composants d'un client Data Protector et que vous n'avez pas exporté le client à partir de la cellule, vous devrez mettre à jour la configuration de la cellule dans le fichier `cell_info` (sur le Gestionnaire de cellule). Pour ce faire, utilisez la commande suivante sur un système dans la cellule, avec la console de cellule installée :

```
/opt/omni/bin/omnicc -update_host <nom_hôte>
```

4 Mise à niveau vers Data Protector A.06.00

Description du chapitre

Ce chapitre décrit les procédures de mise à niveau et de migration de Data Protector.

Présentation de la mise à niveau

Avant de commencer

Avant de mettre à niveau une version de produit existante vers Data Protector A.06.00, tenez compte des éléments suivants :

- Pour en savoir plus sur les plates-formes et versions prises en charge ou non, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.
- Après la mise à niveau, le Gestionnaire de cellule, le Serveur d'installation et tous les clients doivent avoir la même version de Data Protector installée.
- Après la mise à niveau d'un environnement à plusieurs cellules (MoM), la même version de Data Protector doit être installée sur chaque Gestionnaire de cellule.
- Si vous avez une licence permanente pour Data Protector A.05.00, Data Protector A.05.10 ou Data Protector A.05.50, elle peut être utilisée avec Data Protector A.06.00.

  Dans le cas contraire, assurez-vous que vous disposez d'une licence temporaire valable pour une durée de 60 jours à partir de la date d'installation d'origine.

  Pour plus de détails sur la gestion des licences, reportez-vous au Chapitre 5, “Attribution de licences Data Protector,” page 315.

Condition préalable

- Réalisez une sauvegarde du système de Gestionnaire de cellule existant et de la base de données interne (IDB).

Limites

- La mise à niveau de Data Protector A.06.00 est prise en charge uniquement pour Data Protector A.05.00, Data Protector A.05.10 et A.05.50.
- Avec Data Protector A.06.00, vous ne pouvez pas restaurer une sauvegarde de la base de données interne créée avec des versions précédentes de Data Protector. Une fois le Gestionnaire de cellule mis à niveau, sauvegardez la base de données interne avant de continuer à utiliser Data Protector.

- Le changement de plate-forme du Gestionnaire de cellule n'est pas pris en charge dans la version A.06.00 de Data Protector. Les mises à niveau sont prises en charge uniquement sur une même plate-forme de Gestionnaire de cellule (de HP-UX à HP-UX, de Solaris à Solaris et de Windows à Windows).
- La restauration à partir des sauvegardes de la boîte aux lettres unique Microsoft Exchange Server créées avec Data Protector A.05.00 est impossible après la mise à niveau vers Data Protector A.06.00. Vous pouvez cependant restaurer les sauvegardes existantes dans un fichier `.pst` au moyen d'une restauration de système de fichiers.
- Si vous effectuez la mise à niveau vers Data Protector A.06.00 sous Windows et si votre version de Microsoft Installer (MSI) est antérieure à 2.0, le programme d'installation de Data Protector met automatiquement cette dernière à niveau vers la version 2.0. Dans ce cas, Data Protector affichera une remarque à la fin de l'installation, indiquant que MSI a été mis à niveau. Si MSI a été mis à niveau, il est vivement recommandé de redémarrer le système. Consultez le support de Microsoft pour en savoir plus sur les prérequis de MSI 2.0 en fonction des différents systèmes d'exploitation Windows.

  Pour connaître la version de MSI installée sur votre système, cliquez avec le bouton droit sur `c:\winnt\system32\msi.dll` dans l'Explorateur et sélectionnez `Propriétés`. Dans la boîte de dialogue Propriétés, sélectionnez `Version`.

Séquence de mise à niveau

Pour mettre à niveau votre cellule des versions précédentes du produit vers Data Protector A.06.00, procédez comme suit :

1. Mettez à niveau le Gestionnaire de cellule et le Serveur d’installation vers Data Protector A.06.00. La procédure est différente pour les plates-formes UNIX et Windows.

   Notez que vous devez d'abord mettre à niveau le Gestionnaire de cellule dans la cellule actuelle avant de pouvoir mettre à niveau le Serveur d’installation.

   Pour certaines configurations de cellule spécifiques, les noms de fichiers de la base de données IDB doivent être convertis après la mise à niveau du Gestionnaire de cellule. Dans ce cas, un message vous y invitera. Reportez-vous au tableau 4-1 à la page 282 et au tableau 4-2 à la page 284.

2. Mettez à niveau les clients de l'interface graphique utilisateur.
3. Mettez à niveau les clients qui ont une intégration d'application en ligne installée, telle qu'Oracle, SAP R/3, Informix Server, Microsoft SQL Server, Microsoft Exchange Server et autres.
4. Mettez à niveau les clients sur lesquels un Agent de support (MA) est installé. Vous pouvez effectuer des sauvegardes dès que l'Agent de support (MA) est mis à niveau sur tous les clients MA de la même plate-forme que le Gestionnaire de cellule. Pour les clients MA Data Protector A.05.00 et A.05.10, certaines limites s'appliquent. Reportez-vous au tableau 4-1 à la page 282 et au tableau 4-2 à la page 284.

   Pour plus d'informations sur l'impact de la version de l'Agent de disque (DA) sur la sauvegarde et la restauration avant et après la conversion des noms de fichiers de la base de données IDB, reportez-vous à la section “Conversion des noms de fichiers de la base de données IDB” à la page 281.

Mise à niveau dans un environnement MoM

Pour mettre à niveau votre environnement MoM vers Data Protector A.06.00, vous devez dans un premier temps mettre à niveau le système du Gestionnaire MoM. Cela fait, chaque Gestionnaire de cellule des versions précédentes qui n'aurait pas encore été mis à niveau peut accéder à la MMDB centrale et à l'attribution centralisée des licences, et effectuer des sauvegardes, mais les autres fonctionnalités ne sont pas disponibles. Notez que le partage de périphériques entre la cellule MoM Data Protector A.06.00 et les cellules sur lesquelles d'anciennes versions du produit sont installées n'est pas assuré. Pendant la mise à niveau d'un environnement MoM, aucun des Gestionnaires de cellule de l'environnement MoM ne doit fonctionner.

Conversion nécessaire des noms de fichier de la base de données IDB

Dans les versions A.05.50 et A.06.00 de Data Protector, la gestion et l'affichage des noms de fichiers créés avec des paramètres régionaux différents sur des plates-formes différentes ont été améliorés. Ceci nécessite la conversion des noms de fichiers existants de la base de données IDB pour certaines configurations de cellule spécifiques si vous effectuez une mise à niveau à partir de Data Protector A.05.00 ou A.05.10.

La conversion est effectuée sur :

- le Gestionnaire de cellule UNIX dans le cadre de la sauvegarde post-mise à niveau des clients Windows ;
- le Gestionnaire de cellule Windows en processus d'arrière-plan après la mise à niveau du Gestionnaire de cellule.

Si nécessaire, un message vous invitera à effectuer la conversion de la base de données IDB.

UNIX

Sur un Gestionnaire de cellule UNIX, la conversion de la base de données IDB est réalisée dans le cadre des sauvegardes post-mise à niveau des clients Windows

- jusqu'à l'expiration de la période de conversion ou
- jusqu'à ce qu'une sauvegarde complète de tous les clients Windows de la cellule ait été réalisée. Cette étape est très importante et indispensable.

Pour obtenir des données chiffrées sur les performances de la conversion des noms de fichiers, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

Windows

Sur un Gestionnaire de cellule Windows, la conversion de la base de données IDB peut être reportée à une date ultérieure. Toutefois, certaines limites s'appliquent jusqu'à ce qu'elle soit réalisée.

Vous trouverez des informations plus détaillées concernant la conversion des noms de fichier de la base de données IDB sur les Gestionnaires de cellule Windows et UNIX dans la section “Conversion des noms de fichiers de la base de données IDB” à la page 281.

Mise à niveau à partir de Data Protector A.05.x

Les versions de Data Protector A.05.x peuvent être directement mises à niveau vers Data Protector A.06.00 pour les plates-formes UNIX et Windows.

Licences

Les licences existantes de Data Protector A.05.x sont totalement compatibles et valides pour une utilisation avec Data Protector A.06.00. Pour plus de détails sur la gestion des licences, reportez-vous au Chapitre 5, “Attribution de licences Data Protector,” page 315.

Avant de commencer

Avant de commencer la mise à niveau, reportez-vous à la section “Présentation de la mise à niveau” à la page 249 pour plus d'informations sur les limites et la séquence de mise à niveau.

REMARQUE

Les procédures de ce chapitre pour l'installation du Gestionnaire de cellule et du Serveur d’installation et pour l'installation locale des clients supposent l'utilisation d'un DVD-ROM comme support d'installation. Si vous utilisez un support CD-ROM, reportez-vous également à l'“Annexe C,” à la page C-1, dans lequel vous trouverez une liste de CD-ROM et les différences dans la procédure de mise à niveau.

Mise à niveau du Gestionnaire de cellule et du Serveur d’installation UNIX

Configuration requise

- Arrêtez tous les services Data Protector en exécutant la commande `/opt/omni/sbin/omnisv -stop`.
- Sur Solaris, si des anciens correctifs sont installés, désinstallez-les avant la mise à niveau.
- Le Korn Shell (`ksh`) doit être installé.
- Vous devez bénéficier des droits `root` pour effectuer la mise à niveau.

Si le Serveur d'installation HP-UX ou Solaris est installé conjointement avec le Gestionnaire de cellule, il est mis à niveau automatiquement lors de l'exécution de la commande `omnisetup.sh`.

Si le Serveur d'installation HP-UX ou Solaris est installé sur un système distinct, reportez-vous à la section "Mise à niveau d'un Serveur d'installation" à la page 257.

Mise à niveau d'un Gestionnaire de cellule

Le Gestionnaire de cellule HP-UX est mis à niveau automatiquement lorsque la commande `omnisetup.sh` est exécutée.

Sous HP-UX, cette commande met automatiquement à niveau le package existant à l'aide de l'utilitaire `swinstall`. Sous Solaris, cette commande supprime l'ensemble des packages existants à l'aide de l'utilitaire `pkgrm` et installe les nouveaux packages à l'aide de l'utilitaire `pkgadd`.

Si le Serveur d'installation est installé avec des composants client, il sera supprimé par la commande `omnisetup.sh`. Dans ce cas, installez un nouveau dépôt de Serveur d'installation au moyen de la commande `omnisetup.sh -IS`, puis réimportez le Serveur d'installation mis à niveau. Pour plus de détails, reportez-vous à la section "Importation d'un Serveur d'installation dans une cellule" à la page 199.

MC/ServiceGuard

La procédure de mise à niveau du Gestionnaire de cellule configuré sur MC/SG est différente de celle effectuée sur un Gestionnaire de cellule ne fonctionnant pas dans l'environnement MC/SG. La procédure détaillée correspondante est décrite à la section "Mise à niveau du Gestionnaire de cellule configuré sur MC/ServiceGuard" à la page 307.

Définition des paramètres de noyau

Sur les systèmes HP-UX, il est recommandé de définir le paramètre de noyau `maxdsiz` (taille maximale des segments de données) sur au moins 134 217 728 octets (128 Mo), et le paramètre de noyau `semmnu` (nombre de structures Undo de sémaphore) sur au moins 256 Mo. Une fois ces modifications effectuées, recompilez le noyau et redémarrez la machine.

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

Procédure de mise à niveau

Procédez comme suit pour mettre à niveau le Gestionnaire de cellule HP-UX ou Solaris vers Data Protector A.06.00 :

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

   Par exemple :

   ```
   mkdir /dvdrom
   mount /dev/c0d0t0 /dvdrom
   ```

   Si vous souhaitez installer Data Protector depuis un dépôt sur le disque, procédez comme suit :

   - Copiez les répertoires DP_DEPOT, LOCAL_INSTALL et AUTOPASS (où se trouvent les fichiers d'installation) :

     ```
     mkdir <répertoire>
     cp -r /dvdrom/<rép_plateforme>/DP_DEPOT <répertoire>
     cp -r /dvdrom/<rép_plateforme>/AUTOPASS <répertoire>
     cp -r /dvdrom/LOCAL_INSTALL <répertoire>
     ```

     Où *<rép_plateforme>* est :

hpux_ia	HP-UX 11.23 sur les systèmes IA-64
hpux_pa	HP-UX sur les systèmes PA-RISC
solaris	Systèmes Solaris

   - Copiez l'ensemble du DVD-ROM sur votre disque local :

     ```
     cp -r /dvdrom <rép_image_dvd>
     ```

2. Exécutez la commande omnisetup.sh.

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

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

   Pour lancer l'installation à partir du disque :

   - Si vous avez copié les répertoires DP_DEPOT, LOCAL_INSTALL et AUTOPASS sur votre disque local sous *<répertoire>*, allez sur le répertoire qui contient le fichier omnisetup.sh et exécutez la commande suivante :

     ```
     cd <répertoire>/LOCAL_INSTALL
     ./omnisetup.sh
     ```

- Si vous avez copié l'intégralité du DVD-ROM dans *<rép_image_dvd>*, exécutez la commande `omnisetup.sh` sans paramètres :

  ```
  cd <rép_image_dvd>/LOCAL_INSTALL
  ./omnisetup.sh
  ```

3. `omnisetup.sh` vous invite à installer ou à mettre à niveau l'utilitaire HP OpenView AutoPass, si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à la section “Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP OpenView AutoPass” à la page 334. L'installation d'AutoPass est recommandée.

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

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

   Lorsque la version A.05.x de Data Protector est détectée, la procédure de mise à niveau démarre automatiquement. Si vous souhaitez effectuer une installation propre (la version précédente de la base de données sera effacée), désinstallez l'ancienne version puis redémarrez l'installation.

   Pour plus de détails sur la gestion des licences, reportez-vous aux sections “Installation d'un Gestionnaire de cellule UNIX” à la page 21 et “Installation des Serveurs d'installation pour UNIX” à la page 40.

4. Si vous réalisez une mise à niveau de Data Protector A.05.00 ou A.05.10 et que la cellule contient des clients Windows, un message vous informera que la conversion des noms de fichier de la base de données IDB va être réalisée. La conversion de la base de données IDB est nécessaire pour la gestion correcte des noms de fichiers comportant des caractères internationaux. Pour plus de détails, reportez-vous à la section “Conversion des noms de fichiers de la base de données IDB” à la page 281.

Dès que la procédure est terminée, vous pouvez utiliser les fonctionnalités de Data Protector.

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

Etape suivante

Une fois que les systèmes du Gestionnaire de cellule et du Serveur d'installation ont été mis à niveau, vérifiez si vous devez appliquer des modifications à vos fichiers de configuration. Reportez-vous à la section "Vérification des changements de configuration" à la page 264.

Mise à niveau d'un Serveur d'installation

Le Serveur d'installation HP-UX est mis à niveau automatiquement lorsque la commande `omnisetup.sh` est exécutée.

Sous HP-UX, cette commande met automatiquement à niveau le package existant à l'aide de l'utilitaire `swinstall`. Sous Solaris, cette commande supprime l'ensemble des packages existants à l'aide de l'utilitaire `pkgrm` et installe les nouveaux packages à l'aide de l'utilitaire `pkgadd`.

Si le Serveur d'installation est installé avec des composants client, il sera supprimé par la commande `omnisetup.sh`. Dans ce cas, installez un nouveau dépôt de Serveur d'installation au moyen de la commande `omnisetup.sh -IS`, puis réimportez le Serveur d'installation mis à niveau. Pour plus de détails, reportez-vous à la section "Importation d'un Serveur d'installation dans une cellule" à la page 199.

IMPORTANT

Vous ne pouvez pas mettre à niveau le Serveur d'installation si vous n'avez pas au préalable mis à niveau le Gestionnaire de cellule.

Procédure de mise à niveau

Procédez comme suit pour mettre à niveau le Serveur d'installation HP-UX ou Solaris vers Data Protector A.06.00 :

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

   Par exemple :

   ```
   mkdir /dvdrom
   mount /dev/c0d0t0 /dvdrom
   ```

Si vous souhaitez installer Data Protector depuis un dépôt sur le disque, procédez comme suit :

- Pour copier les répertoires `DP_DEPOT` et `LOCAL_INSTALL` (où se trouvent les fichiers d'installation) sur votre disque local, procédez comme suit :

  ```
  mkdir <répertoire>
  cp -r /dvdrom/<rép_plateforme>/DP_DEPOT <répertoire>
  cp -r /dvdrom/<rép_plateforme>/AUTOPASS <répertoire>
  cp -r /dvdrom/LOCAL_INSTALL <répertoire>
  ```

  Où *<rép_platform>* dépend du système d'exploitation et de la plate-forme du processeur sur lesquels vous mettez à niveau Data Protector :

`hpux_ia`	HP-UX 11.23 sur les systèmes IA-64
`hpux_pa`	HP-UX sur les systèmes PA-RISC
`solaris`	Systèmes Solaris

- Pour copier l'ensemble du DVD-ROM sur votre disque local, exécutez la commande :

  ```
  cp -r /dvdrom <rép_image_dvd>
  ```

2. Exécutez la commande `omnisetup.sh`.

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

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

   Pour lancer l'installation à partir du disque, effectuez l'une des étapes suivantes :

   - Si vous avez copié les répertoires `DP_DEPOT` et `LOCAL_INSTALL` sur votre disque local sous *<répertoire>*, allez sur le répertoire qui contient le fichier `omnisetup.sh` et exécutez la commande suivante :

     ```
     cd <répertoire>/LOCAL_INSTALL
     ./omnisetup.sh
     ```

- Si vous avez copié l'intégralité du DVD-ROM dans *<rép_image_dvd>*, exécutez la commande `omnisetup.sh` sans paramètres :

  ```
  cd <rép_image_dvd>/LOCAL_INSTALL
  ./omnisetup.sh
  ```

Dès que la procédure est terminée, vous pouvez utiliser les fonctionnalités de Data Protector.

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

Etape suivante

Une fois que le système du Serveur d'installation a été mis à niveau, vérifiez si vous devez appliquer des modifications à vos fichiers de configuration. Reportez-vous à la section "Vérification des changements de configuration" à la page 264.

Mise à niveau du Gestionnaire de cellule et du Serveur d'installation Windows

Lorsque la version précédente de Data Protector est détectée, le jeu de composants pris en compte par le système d'exploitation est le même que celui qui est installé (sans les composants obsolètes). Le jeu de packages existant est supprimé et le nouveau jeu de packages est installé comme s'il s'agissait d'une nouvelle installation (propre).

Le Serveur d'installation Windows est mis à niveau automatiquement pendant la procédure de mise à niveau s'il installé sur le même système que le Gestionnaire de cellule. L'ancien dépôt du Serveur d'installation est supprimé et, si le composant `Serveur d'installation` est sélectionné pendant l'installation, le nouveau dépôt du Serveur d'installation est copié à sa place.

Si le Serveur d'installation est installé parallèlement au client Data Protector, et si ce client est mis à niveau à distance (à l'aide de l'interface graphique utilisateur de Data Protector), le Serveur d'installation est lui aussi mis à niveau.

IMPORTANT

Réimportez le Serveur d'installation mis à niveau une fois que la procédure d'installation est terminée. Pour plus de détails, reportez-vous à la section “Importation d'un Serveur d'installation dans une cellule” à la page 199.

REMARQUE

Si vous souhaitez mettre à niveau votre système d'exploitation de Windows NT vers une nouvelle version de Windows, vous devez dans un premier temps mettre à niveau le système d'exploitation, puis la version précédente du produit vers Data Protector A.06.00. Pour plus de détails, reportez-vous à la section “Mise à niveau de Windows NT vers une nouvelle version de Windows” à la page 294.

MS Cluster Server

La procédure de mise à niveau du Gestionnaire de cellule fonctionnant dans un environnement MS Cluster Server est différente de celle d'un Gestionnaire de cellule non configuré pour être utilisé avec MS Cluster Server. La procédure détaillée correspondante est décrite à la section “Mise à niveau du Gestionnaire de cellule configuré sur Microsoft Cluster Server” à la page 311.

Procédure de mise à niveau

Procédez comme suit pour mettre à niveau le Gestionnaire de cellule et le Serveur d'installation Windows vers Data Protector A.06.00 :

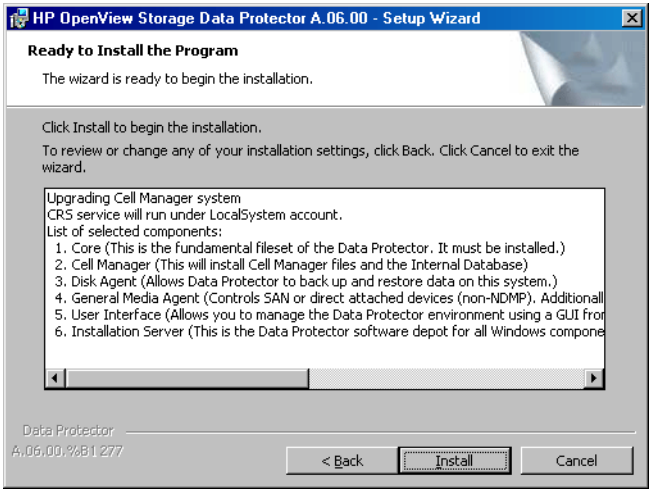
1. Insérez le DVD-ROM d'installation Windows et exécutez la commande `Windows_other\i386\setup.exe`. Le processus d'installation détecte l'ancienne installation de Data Protector. Cliquez sur `Suivant` pour démarrer la mise à niveau.
2. Dans la page `Sélection des composants`, les composants précédemment installés sur le système sont sélectionnés. Notez que vous pouvez modifier le jeu de composants en sélectionnant ou en désélectionnant des composants supplémentaires. Pour obtenir une description des composants sélectionnés, reportez-vous à l'étape suivante de l'assistant. Cliquez sur `Suivant`.
3. ***Windows XP SP2 uniquement*** : si Data Protector détecte le pare-feu Windows sur votre système, la page Configuration du pare-feu Windows est affichée. Data Protector enregistrera tous les exécutables Data Protector nécessaires. Par défaut, l'option

Permettre initialement aux nouveaux fichiers binaires Data Protector enregistrés d'ouvrir des ports le cas échéant est sélectionnée. Si vous ne souhaitez pas activer Data Protector pour les ports ouverts, désélectionnez l'option. Toutefois, notez que les exécutables doivent être activés pour que Data Protector fonctionne correctement.

Cliquez sur `Suivant`.

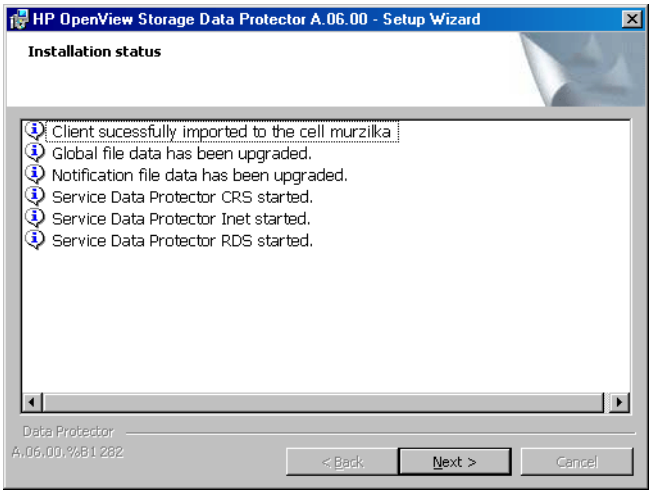
4. La liste des composants sélectionnés s'affiche. Cliquez sur `Installer` pour effectuer la mise à niveau.

Figure 4-1 Page de résumé des composants sélectionnés



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

Figure 4-2 Page d'état de l'installation



6. Si des clients UNIX sont présents dans la cellule, la page `Conversion de l'IDB` s'affiche. Reportez-vous à la section “Conversion des noms de fichiers de la base de données IDB” à la page 281.

7. Cette étape est effectuée uniquement pour la mise à niveau du Gestionnaire de cellule. Si le Serveur d’installation est installé sur un client autre que le Gestionnaire de cellule mis à niveau, cette étape n'apparaît pas.

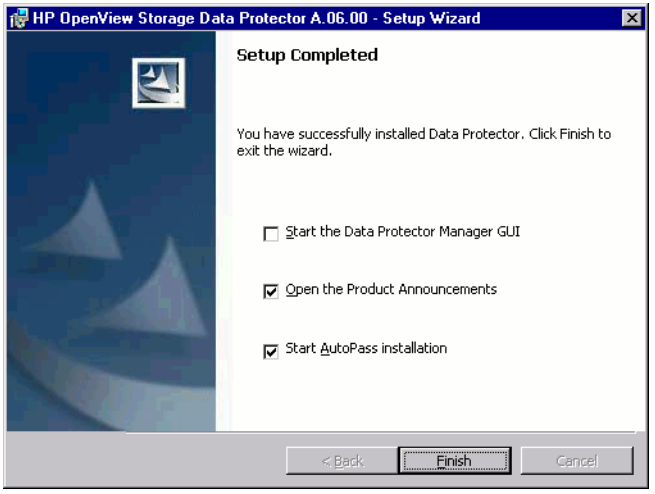
   L'assistant d'installation vous permet d'installer ou de mettre à niveau l'utilitaire HP OpenView Auto Pass, si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à la section “Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP OpenView AutoPass” à la page 334.

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

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

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

Figure 4-3 Sélection de l'installation d'AutoPass



8. Cliquez sur `Terminer`.

Dès que la procédure est terminée, vous pouvez utiliser les fonctionnalités de Data Protector.

Etape suivante

Après la mise à niveau des systèmes du Gestionnaire de cellule et du Serveur d'installation :

- La base de données IDB Data Protector sera convertie si des clients UNIX se trouvent dans la cellule, afin de permettre la gestion correcte des caractères non-ASCII dans les noms de fichiers de Data Protector. Pour plus d'informations sur la conversion de l'IDB, reportez-vous à la section “Conversion des noms de fichiers de la base de données IDB” à la page 281.

- Vérifiez si vous devez appliquer des modifications à vos fichiers de configuration. Reportez-vous à la section “Vérification des changements de configuration” à la page 264.

Vérification des changements de configuration

Fichier d'options globales

Pendant la mise à niveau, le contenu de l'*ancien* fichier d'options globales, qui se trouve dans le répertoire `/etc/opt/omni/options` du Gestionnaire de cellule UNIX ou *<répertoire_Data_Protector>*`\Config\server\Options` du Gestionnaire de cellule Windows, est fusionné avec le contenu du *nouveau* fichier d'options globales sur le Gestionnaire de cellule :

- `/opt/omni/newconfig/etc/opt/omni/server/options` - Gestionnaire de cellule UNIX
- *<répertoire_Data_Protector>*`\NewConfig\Server\Options` - Gestionnaire de cellule Windows

Le fichier *fusionné*, nommé `global`, se trouve dans le répertoire `/etc/opt/omni/server/options` du Gestionnaire de cellule UNIX ou dans le répertoire *<répertoire_Data_Protector>*`\Config\server\Options` du Gestionnaire de cellule Windows, et est utilisé par la version mise à niveau du produit. L'*ancien* fichier d'options globales est renommé en `global.1`, `global.2`, etc., selon le nombre de mises à niveau réalisées.

Les faits suivants s'appliquent après la création du fichier fusionné :

- Les variables du fichier d'options globales qui étaient actives (non mises en commentaires) dans l'ancien fichier restent actives dans le fichier fusionné. Le commentaire suivant, indiquant que la valeur de la variable a été copiée à partir de l'ancien fichier, est ajouté au fichier fusionné :

  <variable>=*<valeur>*

  `# Data Protector A.06.00`

  `# This value was automatically copied from previous version.`

- Les variables du fichier d'options globale qui ne sont plus utilisées sont mises en commentaires (rendues inactives) dans le fichier fusionné ; le commentaire suivant, qui indique que la variable n'est plus utilisée, est ajouté :

  `#` *<variable>*=*<valeur>*

```
# Data Protector A.06.00
# This value is no longer in use.
```

- Les variables dont les valeurs ne sont plus prises en charge sont mises en commentaire (rendues inactives) dans le fichier fusionné. Le commentaire suivant, contenant un modèle (*<modèle_variable>*) et indiquant la valeur précédente de la variable, est inséré :

```
# <variable>=<modèle_variable>
# Data Protector A.06.00
# This variable cannot be transferred automatically.
# The previous setting was:
# <variable>=<valeur>
```

- Les commentaires ne sont pas transférés dans le nouveau fichier fusionné.

Sur les systèmes Windows, le fichier d'options globales est au format UNICODE et peut être modifié avec le Bloc-notes, par exemple. Après avoir modifié ce fichier, veillez à l'enregistrer au format UNICODE.

La description des nouvelles options figure dans le fichier d'options globales fusionné : `/etc/opt/omni/server/options/global` sur un Gestionnaire de cellule UNIX et *<répertoire_Data_Protector>*`\config\server\options\global` sur un Gestionnaire de cellule Windows. La section “Fichier d'options globales” du *Guide de dépannage HP OpenView Storage Data Protector* décrit comment utiliser ces options globales.

Procédure manuelle

La liste ci-dessous récapitule les étapes à réaliser manuellement une fois que la procédure de mise à niveau est terminée :

- Fichier `Omnirc`

  Après la mise à niveau des systèmes du Gestionnaire de cellule et du Serveur d’installation, vous souhaitez peut-être modifier le fichier `omnirc`. Pour obtenir des informations sur la procédure à suivre, reportez-vous à la section relative à l'utilisation du fichier Omnirc dans le *Guide de dépannage HP OpenView Storage Data Protector*.

- Ligne de commande

  Reportez-vous à la section “Modifications de la ligne de commande après la mise à niveau vers Data Protector A.06.00” à la page B-88 pour obtenir une liste des commandes qui ont été modifiées ou

fournies avec des fonctionnalités étendues. Vous devez vérifier et modifier les scripts utilisant les anciennes commandes. Reportez-vous aux pages correspondantes du manuel pour un synopsis d'utilisation.

Etape suivante

Une fois que le Gestionnaire de cellule et le Serveur d'installation sont installés et que toutes les modifications requises ont été appliquées, il est recommandé de distribuer le logiciel aux clients. Reportez-vous à la section "Mise à niveau des clients" à la page 266.

Mise à niveau des clients

Séquence de mise à niveau

Pour plus d'informations sur l'ordre dans lequel la mise à niveau du client est effectuée, reportez-vous à la section "Présentation de la mise à niveau" à la page 249.

Mise à niveau des clients à distance

Pour connaître la procédure de mise à niveau des clients à l'aide du Serveur d'installation, reportez-vous à la section "Installation distante de clients Data Protector" à la page 54. Sur les systèmes UNIX, vous devez mettre à niveau les composants déjà installés avant d'ajouter de nouveaux composants. Après l'ajout de nouveaux composants, Data Protector n'affiche pas les composants des versions précédentes. Dans ce cas, vous devez les réinstaller.

Mise à niveau des clients en local

Si le Serveur d'installation n'est pas installé sur votre réseau ou si, pour une raison quelconque, vous ne pouvez pas distribuer le logiciel Data Protector à un système client, les clients Data Protector peuvent être mis à niveau en local.

Pour mettre à niveau les clients Windows en local, reportez-vous à la section "Installation de clients Windows" à la page 68. Pour mettre à niveau les clients UNIX en local, reportez-vous à la section "Installation locale de clients UNIX" à la page 130.

Novell NetWare

Après la mise à niveau d'un client Novell NetWare, vous devez effectuer quelques étapes supplémentaires qui vous permettront de réaliser toute sauvegarde ou restauration de la base de données NDS/eDirectory. Pour plus de détails, reportez-vous à la section "Installation locale de clients Novell NetWare" à la page 112.

Clients Linux

Lors de la mise à niveau de clients Linux, les fichiers binaires et de configuration Data Protector sont déplacés de `/usr/omni` vers `/opt/omni` (fichiers binaires) ou `/etc/opt/omni` (fichiers de

configuration). Les scripts de pré-exécution et de post-exécution ne sont pas déplacés dans `/opt/omni`, mais ils sont copiés dans `/tmp/usr_omni`. Vous devez les copier manuellement dans `/opt/omni/lbin`.

Si le service `xinetd` est utilisé au lieu de `inetd`, le fichier `/etc/xinetd.d/omni` *n'*est *pas* remplacé et les paramètres demeurent inchangés. Pour vérifier que le service `xinetd` est exécuté, tapez la commande suivante :

```
ps -e | grep xinetd
```

Pour remplacer vos paramètres par les paramètres par défaut de Data Protector ou pour remplacer un fichier endommagé, retirez le fichier et tout composant logiciel Data Protector de l'interface graphique utilisateur de Data Protector. Le fichier `/etc/xinetd.d/omni` est alors installé avec les paramètres par défaut.

IMPORTANT

Le remplacement du fichier `/etc/xinetd.d/omni` entraîne la perte de vos modifications. Si vous souhaitez conserver vos modifications, créez une copie de sauvegarde et transférez les paramètres manuellement vers le nouveau fichier.

Mise à niveau du client configuré sur MC/ServiceGuard

Si vous mettez à niveau le client utilisant MC/ServiceGuard et que le composant d'intégration Data Protector à mettre à niveau est installé sur le même nœud que le Gestionnaire de cellule, mettez à niveau d'abord les nœuds physiques, puis procédez comme suit :

1. Exportez l'hôte virtuel par la commande :

   ```
   omnicc -import_host <nom_hôte_virtuel>
   ```

2. Exportez l'hôte virtuel par la commande :

   ```
   omnicc -import_host <nom_hôte_virtuel> -virtual
   ```

Mise à niveau de clients avec des intégrations

Si vous mettez à niveau le client Data Protector sur lequel l'intégration (par exemple Oracle, SAP R/3, Informix Server, Sybase, Microsoft Exchange Server, HP StorageWorks Disk Array XP, EMC Symmetrix, etc.) est installée, suivez les procédures décrites aux paragraphes ci-dessous :

- Pour obtenir des instructions sur la procédure de mise à niveau de l'intégration Oracle, reportez-vous à la section “Mise à niveau de l'intégration Oracle” à la page 268.
- Pour obtenir des instructions sur la procédure de mise à niveau de l'intégration SAP R/3, reportez-vous à la section “Mise à niveau de l'intégration SAP R/3” à la page 270.
- Pour obtenir des instructions sur la procédure de mise à niveau de l'intégration Informix Server, reportez-vous aux sections “Mise à niveau de l'intégration du serveur Informix sur des systèmes UNIX” à la page 271 et “Mise à niveau de l'intégration du serveur Informix sur des systèmes Windows” à la page 273.
- Pour obtenir des instructions sur la procédure de mise à niveau de l'intégration Sybase, reportez-vous aux sections “Mise à niveau de l'intégration Sybase sur des systèmes UNIX” à la page 274 et “Mise à niveau de l'intégration Sybase sur des systèmes Windows” à la page 275.
- Pour obtenir des instructions sur les procédures de mise à niveau des intégrations MS Exchange, MS SQL, HP StorageWorks Disk Array XP, EMC Symmetrix, etc., reportez-vous à la section “Mise à niveau des autres intégrations” à la page 279.

Mise à niveau de l'intégration Oracle

Les clients sur lesquels l'intégration Oracle est installée sont mis à niveau soit localement par la commande `omnisetup.sh -install oracle8` sur les systèmes UNIX ou `setup.exe` sur les systèmes Windows, soit à distance en chargeant l'agent d'intégration Oracle sur le client à l'aide de l'interface graphique de Data Protector. Sous UNIX, notez que si vous mettez à niveau le client qui ne réside pas sur le Gestionnaire de cellule, il n'est pas nécessaire de spécifier l'option `-install oracle8`. Dans ce cas, le programme d'installation sélectionnera sans émettre d'invite les mêmes composants que ceux déjà installés sur le système.

Nouveaux modèles après la mise à niveau Si vous effectuez une mise à niveau à partir de Data Protector A.05.00 ou A.05.10, les modèles Oracle sont remplacés par des versions plus récentes. Les nouveaux modèles se trouvent dans le répertoire suivant :

`/opt/omni/newconfig/etc/opt/omni/server/dltemplates/lists/oracle8` (sur les systèmes UNIX) ou `<répertoire_Data_Protector>\NewConfig\server\dltemplates\lists\oracle8` (sur les systèmes Windows).

Pour utiliser les nouveaux modèles, copiez-les après la mise à niveau vers Data Protector A.06.00 dans le répertoire `/etc/opt/omni/server/dltemplates/lists\oracle8` (sur les systèmes UNIX) ou `<répertoire_Data_Protector>\Config\server\dltemplates\lists\oracle8` (sur les systèmes Windows). Si vous souhaitez conserver les anciens modèles, enregistrez-les sous un autre nom.

Configuration de la méthode ZDB Selon que le fichier de configuration de l'instance Oracle contient ou non le paramètre *<ORACLE_DBID>*, le fichier de configuration de méthode ZDB est défini pour Data Protector A.06.00 comme suit :

- Si le fichier de configuration de l'instance Oracle contient le paramètre *<ORACLE_DBID>* (dans Data Protector A.05.10 et A.05.50), le fichier de configuration de méthode ZDB est créé pour chaque instance de la base de données *pendant la mise à niveau*.
- Si le fichier de configuration de l'instance Oracle *ne* contient *pas* le paramètre *<ORACLE_DBID>* (Data Protector A.05.00), le fichier de configuration de méthode ZDB est créé pour chaque instance *pendant la première session de sauvegarde*.

La méthode ZDB Oracle n'est pas modifiée pendant la mise à niveau. Pour plus d'informations sur la commutation entre les méthodes ZDB de proxy-copy et de jeu de sauvegardes, reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

Mise à niveau ZDB Oracle Si vous effectuez une mise à niveau à partir de Data Protector A.05.00 ou A.05.10, les spécifications de sauvegarde ZDB Oracle sont automatiquement mises à niveau à la fin d'une procédure standard de mise à niveau de l'intégration Oracle.

Les opérations suivantes sont effectuées au cours d'une mise à niveau des spécifications de sauvegarde :

- Les paramètres `OB2DMAP` et `OB2SMB` sont ajoutés à la *première* commande RMAN `ALLOCATE CHANNEL`. Le paramètre `OB2DMAP` est configuré en fonction du nombre de canaux alloués avant la mise à niveau. Par exemple, dans le cas d'un script RMAN comprenant 4 canaux alloués, le paramètre `OB2DMAP` est défini sur 4.
- Toutes les commandes `ALLOCATE CHANNEL`, excepté la première, sont supprimées des scripts.
- Si la restauration instantanée est activée, les objets sauvegarde `TABLESPACE` ou `DATAFILES` sont changés en `DATABASE` pour permettre des sauvegardes uniquement de l'intégralité de la base de données.
- Si la méthode de sauvegarde proxy-copy a été utilisée, toutes les commandes `RELEASE CHANNEL` sont supprimées à l'exception de celle qui fait référence à la première commande `ALOCATE CHANNEL`.

Pour plus de détails, reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector pour Oracle et SAP* ou au *Guide d'intégration HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

Configuration d'une instance d'Oracle pour la restauration instantanée Si les fichiers de contrôle, les catalogues de récupération ou les journaux de rétablissement archivés se trouvent dans le même groupe de volumes (si LVM est utilisé) ou dans le même volume source que les fichiers de base de données, vous devez reconfigurer l'instance d'Oracle ou définir les variables `omnirc` `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

Mise à niveau de l'intégration SAP R/3

Les clients sur lesquels l'intégration SAP R/3 est installée sont mis à niveau soit localement par la commande `omnisetup.sh -install sap` sur les systèmes UNIX ou `setup.exe` sur les systèmes Windows, soit à distance en chargeant l'agent d'intégration SAP R/3 sur le client à l'aide de l'interface graphique de Data Protector. Sous UNIX, notez que si vous mettez à niveau le client qui ne réside pas sur le Gestionnaire de cellule,

il n'est pas nécessaire de spécifier l'option `-install sap`. Dans ce cas, le programme d'installation sélectionnera sans émettre d'invite les mêmes composants que ceux déjà installés sur le système.

Configuration d'une instance d'Oracle pour la restauration instantanée Si les fichiers de contrôle, les catalogues de récupération ou les journaux de rétablissement archivés se trouvent dans le même groupe de volumes (si LVM est utilisé) ou dans le même volume source que les fichiers de base de données, vous devez reconfigurer l'instance d'Oracle ou définir les variables `omnirc ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Reportez-vous au *Guide d'intégration HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.

Mise à niveau de l'intégration du serveur Informix sur des systèmes UNIX

Lorsque vous mettez à niveau l'intégration du serveur Informix de Data Protector A.05.00 et A.05.10 vers Data Protector A.06.00, il existe trois procédures de mise à niveau, en fonction de l'environnement :

Procédure 1 Si le client du serveur Informix *ne se trouve pas* sur le même système que le Gestionnaire de cellule et s'il *n'est pas configuré* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Informix Data Protector sont automatiquement déplacés d'un client du serveur Informix Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Aucune reconfiguration des bases de données du serveur Informix n'est nécessaire après la mise à niveau.

Mettez le client à niveau, soit localement par la commande `omnisetup.sh`, soit à distance en chargeant l'agent d'intégration du serveur Informix sur le client avec l'interface graphique de Data Protector.

Procédure 2 Si le client du serveur Informix *ne se trouve pas* sur le même système que le Gestionnaire de cellule et s'il *est configuré* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Informix Data Protector sont automatiquement déplacés du client du

serveur Informix Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Après la mise à niveau, les bases de données du serveur Informix doivent être reconfigurées.

1. Mettez le client à niveau, soit localement par la commande `omnisetup.sh`, soit à distance en chargeant l'agent d'intégration du serveur Informix sur le client avec l'interface graphique de Data Protector.
2. Configurez les bases de données du serveur Informix à l'aide de l'interface graphique ou de l'interface de ligne de commande Data Protector selon les indications du *Guide d'intégration HP OpenView Storage Data Protector*.

   Configurez les bases de données du serveur Informix à l'aide du nom d'hôte virtuel du serveur Informix.

Procédure 3

Si le client du serveur Informix *se trouve* sur le même système qu'un Gestionnaire de cellule *compatible cluster* et s'il est *configuré ou non* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Informix Data Protector ne sont pas automatiquement déplacés du client du serveur Informix Data Protector vers le Gestionnaire de cellule pendant la mise à niveau. Après la mise à niveau, les bases de données du serveur Informix doivent être reconfigurées.

1. Mettez le client à niveau, soit localement par la commande `omnisetup.sh`, soit à distance en chargeant l'agent d'intégration du serveur Informix sur le client avec l'interface graphique de Data Protector.

2. Configurez les bases de données du serveur Informix à l'aide de l'interface graphique ou de l'interface de ligne de commande Data Protector selon les indications du *Guide d'intégration HP OpenView Storage Data Protector*.

Mise à niveau de l'intégration du serveur Informix sur des systèmes Windows

Lorsque vous mettez à niveau l'intégration du serveur Informix de Data Protector A.05.00 et A.05.10 vers Data Protector A.06.00, il existe trois procédures de mise à niveau, en fonction de l'environnement :

Procédure 1

Si le client du serveur Informix *ne se trouve pas* sur le même système que le Gestionnaire de cellule et s'il *n'est pas configuré* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Informix Data Protector sont automatiquement déplacés du client du serveur Informix Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Aucune reconfiguration des bases de données du serveur Informix n'est nécessaire après la mise à niveau.

Mettez le client à niveau, soit localement par la commande `setup.exe`, soit à distance en chargeant l'agent d'intégration du serveur Informix sur le client avec l'interface graphique de Data Protector.

Procédure 2

Si le client du serveur Informix *ne se trouve pas* sur le même système que le Gestionnaire de cellule et s'il *est configuré* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Informix Data Protector sont automatiquement déplacés du client du serveur Informix Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Après la mise à niveau, les bases de données du serveur Informix doivent être reconfigurées.

1. Mettez le client à niveau, soit localement par la commande `setup.exe`, soit à distance en chargeant l'agent d'intégration du serveur Informix sur le client avec l'interface graphique de Data Protector.
2. Configurez les bases de données du serveur Informix à l'aide de l'interface graphique ou de l'interface de ligne de commande de Data Protector selon les indications du *Guide d'intégration HP OpenView Storage Data Protector*.

   Configurez les bases de données du serveur Informix à l'aide du nom d'hôte virtuel du serveur Informix.

Procédure 3

Si le client du serveur Informix *se trouve* sur le même système qu'un Gestionnaire de cellule *compatible cluster* et s'il est *configuré ou non* comme client Data Protector compatible cluster, les paramètres de configuration du serveur Informix Data Protector ne sont pas automatiquement déplacés du client du serveur Informix Data Protector vers le Gestionnaire de cellule pendant la mise à niveau. Après la mise à niveau, les bases de données du serveur Informix doivent être reconfigurées.

1. Mettez le client à niveau, soit localement par la commande `setup.exe`, soit à distance en chargeant l'agent d'intégration du serveur Informix sur le client avec l'interface graphique de Data Protector.
2. Configurez les bases de données du serveur Informix à l'aide de l'interface graphique ou de l'interface de ligne de commande de Data Protector selon les indications du *Guide d'intégration HP OpenView Storage Data Protector*.

Mise à niveau de l'intégration Sybase sur des systèmes UNIX

Lorsque vous mettez à niveau l'intégration Sybase de Data Protector A.05.00 et A.05.10 vers Data Protector A.06.00, il existe trois procédures de mise à niveau, en fonction de l'environnement :

Procédure 1

Si le client Sybase *ne se trouve pas* sur le même système que le Gestionnaire de cellule et qu'il *n'est pas configuré* comme client Data Protector compatible cluster, les paramètres de configuration Sybase Data Protector sont automatiquement déplacés du client Sybase Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Aucune reconfiguration du serveur Sybase n'est nécessaire après la mise à niveau.

Mettez le client à niveau, soit localement par la commande `omnisetup.sh`, soit à distance en chargeant l'agent d'intégration Sybase sur le client avec l'interface graphique de Data Protector.

Procédure 2

Si le client Sybase *ne se trouve pas* sur le même système que le Gestionnaire de cellule et qu'il *est configuré* comme client Data Protector compatible cluster, les paramètres de configuration Sybase Data Protector sont automatiquement déplacés du client Sybase Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Après la mise à niveau, le serveur Sybase doit être reconfiguré.

1. Mettez le client à niveau, soit localement par la commande `omnisetup.sh`, soit à distance en chargeant l'agent d'intégration Sybase sur le client avec l'interface graphique de Data Protector.
2. Configurez le client Sybase au moyen de l'interface graphique ou de l'interface de ligne de commande de Data Protector comme expliqué dans le *Guide d'intégration HP OpenView Storage Data Protector*.

   Configurez le serveur Sybase à l'aide du nom d'hôte virtuel du serveur Sybase.

Procédure 3

Si le client Sybase *se trouve* sur le même système qu'un *Gestionnaire de cellule compatible cluster* et qu'il *est configuré ou non* comme client Data Protector compatible cluster, les paramètres de configuration Sybase Data Protector ne sont pas automatiquement déplacés du client Sybase Data Protector vers le Gestionnaire de cellule pendant la mise à niveau. Après la mise à niveau, le serveur Sybase doit être reconfiguré.

1. Mettez le client à niveau, soit localement par la commande `omnisetup.sh`, soit à distance en chargeant l'agent d'intégration Sybase sur le client avec l'interface graphique de Data Protector.
2. Configurez le serveur Sybase au moyen de l'interface graphique ou de l'interface de ligne de commande de Data Protector comme expliqué dans le *Guide d'intégration HP OpenView Storage Data Protector*.

   Si le serveur Sybase est configuré comme client Data Protector compatible cluster, configurez-le en utilisant le nom d'hôte virtuel du serveur en ligne.

   Si le serveur Sybase n'est pas configuré comme client Data Protector compatible cluster, configurez-le en utilisant le nom d'hôte du serveur Sybase.

Mise à niveau de l'intégration Sybase sur des systèmes Windows

Lorsque vous mettez à niveau l'intégration Sybase de Data Protector A.05.00 et A.05.10 vers Data Protector A.06.00, il existe trois procédures de mise à niveau, en fonction de l'environnement :

Procédure 1

Si le client Sybase *ne se trouve pas* sur le même système que le Gestionnaire de cellule et qu'il *n'est pas configuré* comme client Data Protector compatible cluster, les paramètres de configuration Sybase Data Protector sont automatiquement déplacés du client Sybase Data

Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Aucune reconfiguration du serveur Sybase n'est nécessaire après la mise à niveau.

Mettez le client à niveau, soit localement par la commande `setup.exe`, soit à distance en chargeant l'agent d'intégration Sybase sur le client avec l'interface graphique de Data Protector.

Procédure 2

Si le client Sybase *ne se trouve pas* sur le même système que le Gestionnaire de cellule et qu'il *est configuré* comme client Data Protector compatible cluster, les paramètres de configuration Sybase Data Protector sont automatiquement déplacés du client Sybase Data Protector vers le Gestionnaire de cellule au cours de la mise à niveau. Après la mise à niveau, le serveur Sybase doit être reconfiguré.

1. Mettez le client à niveau, soit localement par la commande `setup.exe`, soit à distance en chargeant l'agent d'intégration Sybase sur le client avec l'interface graphique de Data Protector.
2. Configurez le client Sybase au moyen de l'interface graphique ou de l'interface de ligne de commande de Data Protector comme expliqué dans le *Guide d'intégration HP OpenView Storage Data Protector*.

   Configurez le serveur Sybase à l'aide du nom d'hôte virtuel du serveur SQL Sybase.

Procédure 3

Si le client Sybase *se trouve* sur le même système qu'un *Gestionnaire de cellule compatible cluster* et qu'il *est configuré ou non* comme client Data Protector compatible cluster, les paramètres de configuration Sybase Data Protector ne sont pas automatiquement déplacés du client Sybase Data Protector vers le Gestionnaire de cellule pendant la mise à niveau. Après la mise à niveau, le serveur Sybase doit être reconfiguré.

1. Mettez le client à niveau, soit localement par la commande `setup.exe`, soit à distance en chargeant l'agent d'intégration Sybase sur le client avec l'interface graphique de Data Protector.
2. Configurez le client Sybase au moyen de l'interface graphique ou de l'interface de ligne de commande de Data Protector comme expliqué dans le *Guide d'intégration HP OpenView Storage Data Protector*.

   Si le serveur Sybase est configuré comme client Data Protector compatible cluster, configurez-le en utilisant le nom d'hôte virtuel du serveur en ligne.

Si le serveur Sybase n'est pas configuré comme client Data Protector compatible cluster, configurez-le en utilisant le nom d'hôte du serveur Sybase.

Mise à niveau de l'intégration de HP StorageWorks EVA

La mise à niveau de l'intégration de HP StorageWorks EVA s'effectue à partir de l'Agent HP StorageWorks EVA (hérité) vers l'Agent HP StorageWorks EVA SMI-S. Cette mise à niveau est nécessaire en raison du caractère obsolète de l'agent EVA (hérité).

Si la procédure de mise à niveau s'est déroulée correctement, les résultats sont les suivants :

- Mise à niveau des spécifications de sauvegarde créées par l'Agent EVA (hérité)
- Transfert des informations sur les sessions de sauvegarde de l'EVADB vers la SMISDB afin de permettre leur restauration par l'Agent SMI-S
- Transfert des règles de groupes de disques et de connexion définies pour l'Agent EVA (existant) vers la SMISDB

Pour obtenir des informations détaillées sur les versions des produits associés prises en charge, ainsi qu'une liste des plates-formes sur lesquelles l'Agent SMI-S est pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

Conditions préalables

- Veillez à satisfaire les conditions minimales requises pour les systèmes d'exploitation sur lesquels l'agent SMI-S est pris en charge.
- Aucune sauvegarde EVA ne doit être en cours d'exécution. La procédure de mise à niveau peut faire échouer la sauvegarde ; dans ce cas, aucune information de session ne s'affichera dans la SMIDB et il sera impossible d'effectuer une restauration à partir de cette session.
- Ne lancez la mise à niveau d'un agent qu'une fois la mise à niveau du Gestionnaire de cellule terminée.

Procédure de mise à niveau

Pour effectuer une mise à niveau de l'Agent HP StorageWorks EVA (hérité) vers l'Agent HP StorageWorks EVA SMI-S, suivez les étapes décrites ci-dessous :

1. Sur le Gestionnaire de cellule, exécutez la commande `upgrade_cm_from_evaa` afin de mettre à niveau toutes les entrées EVADB vers les entrées SMISDB. Exécutez cette commande seulement lorsque la mise à niveau du Gestionnaire de cellule est terminée.

   Les informations suivantes sont transférées :

   - Spécifications de sauvegarde et sessions de sauvegarde (répliques) créées par l'Agent EVA (hérité)
   - Entrées de connexion associées au système de gestion EVA

   Prenez en compte les points suivants :

Connexion

   - Si une entrée de connexion est déjà présente dans la SMISDB, aucune nouvelle entrée n'est créée pour ce système de gestion.
   - Les nom d'utilisateur et mot de passe de connexion sont supposés être les mêmes pour CV EVA et un fournisseur SMI-S.
   - L'entrée de connexion SMISDB utilisera toujours le port 5988.

Règles de groupes de disques

   - S'il existe déjà une règle pour un groupe de disques donné dans la SMISDB, aucune mise à jour n'est effectuée.
   - Toutes les règles de groupes de disques définies pour l'Agent EVA (hérité) sont ajoutées à la suite des règles de groupes de disques SMISDB existantes.

   Pour plus d'informations su la commande `upgrade_cm_from_evaa`, reportez-vous au document *Référence de l'interface de ligne de commande HP OpenView Storage Data Protector*.

2. Sur le système d'application, exécutez la commande `omnisetup.sh -install smisa` sur les systèmes UNIX ou la commande `setup.exe` sur les systèmes Windows si vous effectuez une mise à niveau locale. Si vous effectuez une mise à niveau à distance, chargez (push) l'Agent EVA SMI-S sur le client à l'aide de l'assistant `Ajouter composants` de l'interface graphique et sélectionnez `Agent HP StorageWorks EVA SMI-S`.

Ce script de pré-exécution vérifie si le package EVAA se trouve sur le système. Si le package est détecté, les informations relatives à ce dernier sont supprimées du Gestionnaire de cellule.

Parallèlement à la désinstallation du package EVAA, les informations relatives aux sessions de sauvegarde EVA (répliques) créées par l'Agent EVA (hérité) sont transférées de l'EVADB à la SMISDB. Cela signifie qu'après la mise à niveau, vous serez en mesure de restaurer les sessions de sauvegarde créées par l'Agent EVA (hérité) à l'aide de l'Agent SMI-S.

3. Une fois le système d'application mis à niveau, vous devez également mettre à niveau le système de sauvegarde. Les spécifications de sauvegardes planifiées ne fonctionneront pas tant que les systèmes d'application et les systèmes de sauvegarde n'auront pas été mis à niveau.
4. Vérifiez manuellement le fichier `omnirc` afin de vous assurer que les variables `omnirc` ont été correctement mises à niveau.

Mise à niveau des autres intégrations

Si une intégration MS Exchange, MS SQL, HP StorageWorks Disk Array XP, EMC Symmetrix, etc. est installée sur le client Data Protector, mettez ce dernier à niveau, soit localement via la commande `omnisetup.sh -install <liste_composants>` sur les systèmes UNIX ou `setup.exe` sur les systèmes Windows, soit à distance avec l'interface graphique de Data Protector. Pour obtenir une liste des codes des composants Data Protector, reportez-vous à la section “Installation locale de clients UNIX” à la page 130. Notez que si vous mettez à niveau le client qui ne réside pas sur le Gestionnaire de cellule, il n'est pas nécessaire de spécifier l'option `-install <liste_composants>`. Dans ce cas, le programme d'installation sélectionnera sans émettre d'invite les mêmes composants que ceux déjà installés sur le système.

Mise à niveau dans un environnement MoM

Vous pouvez mettre à niveau un environnement MoM de manière séquentielle. Toutefois, gardez à l'esprit les limites suivantes :

- Après avoir effectué une mise à niveau du Gestionnaire MoM/serveur CMMDB, il n'est pas possible de procéder à la *restauration* d'un système de fichiers ou d'une intégration Data Protector A.05.x via

l'interface graphique utilisateur MoM Data Protector A.06.00. Par conséquent, utilisez l'ancienne interface graphique utilisateur MoM pour la restauration ou mettez à niveau les clients.

Vous pouvez effectuer une *sauvegarde* de systèmes de fichiers et d'intégrations de clients Data Protector A.05.x via l'interface graphique utilisateur MoM Data Protector A.06.00.

Pour mettre à niveau votre environnement MoM vers Data Protector A.06.00, procédez comme suit :

1. Mettez à niveau le Gestionnaire MoM/serveur CMMDB vers Data Protector A.06.00.

   Aucun Gestionnaire de cellule de l'environnement MoM ne doit fonctionner pendant la mise à niveau. Après la mise à niveau, le Gestionnaire MoM peut toujours fonctionner avec les anciens Gestionnaires de cellule.

2. Mettez à niveau chaque Gestionnaire de cellule client dans un environnement MoM.

   Pour connaître la procédure de mise à niveau à suivre, reportez-vous aux sections “Mise à niveau du Gestionnaire de cellule et du Serveur d’installation UNIX” à la page 253 et “Mise à niveau du Gestionnaire de cellule et du Serveur d’installation Windows” à la page 259.

3. Mettez à niveau les clients avec des périphériques configurés.

4. Mettez à niveau les clients avec des intégrations d'applications.

   Une fois que cette partie de la mise à niveau est effectuée, vous pouvez sauvegarder et restaurer les systèmes de fichiers et les intégrations via l'interface graphique utilisateur MoM Data Protector A.06.00.

Conversion des noms de fichiers de la base de données IDB

Data Protector A.05.50 et A.06.00 présentent une amélioration dans la gestion et l'affichage des noms de fichiers créés avec des paramètres régionaux différents sur des plates-formes différentes. Ceci nécessite la conversion des noms de fichiers existants de la base de données IDB pour certaines configurations de cellule spécifiques si vous effectuez une mise à niveau à partir de Data Protector A.05.00 ou A.05.10. Si vous effectuez une mise à niveau à partir de A.05.50, aucune conversion n'est requise.

La conversion des noms de fichiers de la base de données IDB doit être effectuée. Dans le cas contraire, la navigation et la sélection pour restauration des noms de fichiers contenant des caractères non-ASCII dépend de nombreux facteurs. La probabilité d'obtenir des résultats indésirables est élevée.

La conversion est réalisée :

- sur le Gestionnaire de cellule UNIX dans le cadre de la sauvegarde post-mise à niveau des clients Windows ;
- sur le Gestionnaire de cellule Windows en processus d'arrière-plan après la mise à niveau du Gestionnaire de cellule.

Si nécessaire, un message vous invitera à effectuer la conversion de la base de données IDB.

Le tableau 4-1 à la page 282 (pour le Gestionnaire de cellule Windows) et le tableau 4-2 à la page 284 décrivent l'impact de la conversion de noms de fichier sur le Gestionnaire de cellule si vous effectuez une mise à niveau à partir de Data Protector A.05.00 ou A.05.10.

Tableau 4-1 Impact de la conversion de noms de fichier sur un Gestionnaire de cellule Windows

	UNIX et autres clients	Clients Windows
Requiert une conversion de l'IDB	Oui[1]	Non
Sauvegarde avant la conversion, pas de mise à niveau du client	Problématique[2] Tout client comportant des caractères non ASCII dans ses spécifications de sauvegarde (arborescences, listes d'exclusion, etc.) doit être mis à niveau vers Data Protector A.06.00. Data Protector consigne tous ces clients dans le Journal d'événements Data Protector pendant la mise à niveau pour vous aider à organiser vos tâches de mise à niveau en fonction de leur priorité.	Aucun problème
Sauvegarde avant la conversion, mise à niveau du client vers la version A.06.00	Aucun problème Si un client est sauvegardé alors que la conversion est en cours et si des données IDB de ce client sont converties, la sauvegarde bascule en mode `Pas de journalisation` pour la session concernée.	Aucun problème

Tableau 4-1 Impact de la conversion de noms de fichier sur un Gestionnaire de cellule Windows

	UNIX et autres clients	Clients Windows
Affichage des fichiers à restaurer avant la conversion, sélection des noms de fichier/arborescences non-ASCII à restaurer	Problématique[3] L'affichage correct (et la sélection destinée à la restauration) de caractères non ASCII dans l'interface graphique utilisateur de Data Protector est impossible tant que les noms de fichier dans l'IDB du client concerné ne sont pas convertis.	Aucun problème
Sauvegarde après la conversion	Aucun problème Le client doit être mis à niveau vers Data Protector A.06.00.	Aucun problème
Affichage et restauration des fichiers après la conversion	Aucun problème Le client doit être mis à niveau vers Data Protector A.06.00.	Aucun problème
Compatibilité de l'Agent de disque (versions antérieures)[4]	Data Protector A.05.00 = Non, A.05.10 = Non, A.05.50 = OUI[4].	Data Protector A.05.00 = OUI[4], A.05.10 = OUI [4], A.05.50.= OUI.[4]

Tableau 4-2 Impact de la conversion de noms de fichier sur un Gestionnaire de cellule UNIX

	UNIX et autres clients	Clients Windows
Requiert une conversion de l'IDB	Non	Oui[1]
Sauvegarde pendant la période de conversion, pas de mise à niveau du client	Aucun problème	Problématique[2] Tout client comportant des caractères non ASCII dans ses spécifications de sauvegarde (arborescences, listes d'exclusion, etc.) doit être mis à niveau vers Data Protector A.06.00. Data Protector consigne tous ces clients dans le Journal d'événements Data Protector pour vous aider à organiser vos tâches de mise à niveau en fonction de leur priorité.
Sauvegarde pendant la période de conversion, mise à niveau du client vers la version A.06.00	Aucun problème	Aucun problème Notez que la sauvegarde des clients Windows pendant la période de conversion est nécessaire. Les données de l'IDB de chaque client sont automatiquement converties pendant la sauvegarde du client. Vous devez réaliser une sauvegarde complète pour convertir tous les noms de fichier stockés dans l'IDB du client concerné.

Tableau 4-2 Impact de la conversion de noms de fichier sur un Gestionnaire de cellule UNIX

	UNIX et autres clients	Clients Windows
Affichage des fichiers à restaurer avant la conversion, sélection des noms de fichier/arborescences non ASCII à restaurer	Aucun problème	Problématique[3] L'affichage correct (et la sélection destinée à la restauration) de caractères non ASCII dans l'interface graphique utilisateur de Data Protector est impossible tant qu'une sauvegarde complète n'aura pas été réalisée après la mise à niveau du Gestionnaire de cellule.
Sauvegarde après la période de conversion	Aucun problème	Aucun problème Le client doit être mis à niveau vers Data Protector A.06.00.
Affichage et restauration des fichiers après la conversion	Aucun problème	Aucun problème Le client doit être mis à niveau vers Data Protector A.06.00.
Compatibilité de l'Agent de disque (versions antérieures)[4]	Data Protector A.05.00 = OUI[4], A.05.10 = OUI[4], A.05.50.= OUI[4]	Data Protector A.05.00 = Non, A.05.10 = Non, A.05.50 = OUI[4].

1. Si la conversion de noms de fichier n'est pas réalisée, le nombre de noms de fichier de la partie base de données catalogue (CDB) de l'IDB augmente conformément au nombre de noms de fichier contenant des caractères non ASCII dans les fichiers sauvegardés. Les fichiers et répertoires qui requièrent d'être convertis mais qui ne l'ont pas encore été ne peuvent pas être sélectionnés pour la restauration. Le seul moyen de les restaurer consiste à restaurer une arborescence parente contenant uniquement des caractères ASCII dans un emplacement temporaire.
2. Les restrictions ne s'appliquent pas si les noms de fichier (arborescences) de la spécification de sauvegarde ne contiennent que des caractères ASCII. Si tel est le cas, tous les fichiers et répertoires d'une arborescence sont sauvegardés et leurs noms stockés correctement dans l'IDB même si les noms de fichier (arborescences) contiennent des caractères non ASCII.
3. Les restrictions ne s'appliquent pas si le nom de fichier (arborescence) que vous restaurez ne contient que des caractères ASCII. Dans le cas contraire, vous pouvez le restaurer en restaurant une arborescence parente contenant uniquement des caractères ASCII dans un emplacement temporaire. Tous les fichiers et répertoires de cette arborescence parente seront sauvegardés avec leurs noms de fichier d'origine (même s'ils ne s'affichent pas correctement dans l'interface graphique utilisateur de Data Protector GUI), à condition qu'ils soient restaurés sur leur plate-forme initiale.
4. La prise en charge de l'Agent de disque émanant de versions antérieures est limitée à deux semaines. Pendant ce délai, vous devez mettre à niveau tous les clients de la cellule.

Remarques

- Indépendamment des problèmes de gestion de noms de fichiers, lorsqu'un fichier est sauvegardé et restauré, la séquence d'octets d'origine composant le corps du fichier est conservée.
- Seuls les noms de fichier composés de caractères ASCII 7 bits sont entièrement pris en charge sur toutes les combinaisons de plates-formes et pour tous les composants (Gestionnaire de cellule, client, interface graphique utilisateur). Pour les noms de fichiers comportant des caractères non-ASCII, une configuration et un paramétrage spécifiques sont requis pour que les noms de fichiers soient correctement gérés.

La conversion de la base de données IDB peut demander un certain temps et monopoliser des ressources système, en fonction de la taille de la partie de l'IDB consacrée aux noms de fichier et de la configuration de la cellule. Toutefois, cela n'affecte pas la réussite de vos opérations de sauvegarde ou de restauration.

Conversion de l'IDB dans un Gestionnaire de cellule sous Windows

Introduction

Cette section s'applique aux Gestionnaires de cellule sous Windows dont la cellule contient des clients non-Windows et qui font l'objet d'une mise à niveau à partir de Data Protector A.05.00 ou A.05.10. Si vous effectuez une mise à niveau à partir de A.05.50, aucune conversion n'est requise.

La conversion de l'IDB demande un certain temps, selon sa taille et la configuration de votre cellule ; toutefois, cela n'affecte pas la réussite de vos opérations de sauvegarde ou de restauration. La conversion est effectuée en arrière-plan en une seule passe pour tous les clients non-Windows de la cellule, tandis que Data Protector reste totalement opérationnel. L'intégralité des données d'un client est convertie avant le passage aux données du client suivant. Une fois terminée, la conversion de l'IDB est complète et ne doit pas être répétée.

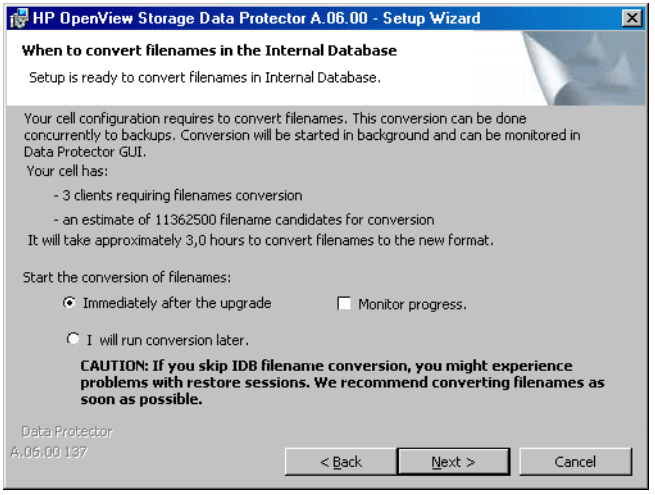
Si les noms de fichier ne comprennent pas de caractères non-ASCII, la conversion de l'IDB s'effectue malgré tout, mais rien ne change dans l'IDB.

La conversion de l'IDB n'affecte pas la taille de la base IDB.

Comment est effectuée la conversion de l'IDB ?

Une fois la mise à niveau de Data Protector terminée, l'assistant d'installation de Data Protector vous propose de convertir les noms de fichier dans l'IDB.

Figure 4-4 Conversion de l'IDB après mise à niveau



Vous obtenez une estimation approximative de la durée de la conversion de l'IDB. Cette estimation est basée sur le nombre de clients non-Windows présents dans la cellule et sur le nombre de fichiers de ces clients qui sont stockés dans l'IDB.

Si vous remettez la conversion à une date ultérieure, vous devrez effectuer manuellement la conversion de l'IDB à l'aide de la commande `omnidbupgrade`. Pour plus de détails, reportez-vous au document *Référence de l'interface de ligne de commande HP OpenView Storage Data Protector*.

REMARQUE Il est recommandé de procéder dès que possible à la conversion de l'IDB et à la mise à niveau des Agents de disque sur les clients.

Vous pouvez contrôler l'état de la conversion de l'IDB (savoir quels sont les clients dont les données ont déjà été converties) dans le menu contextuel `Moniteur` de l'interface utilisateur de Data Protector.

Sauvegarde pendant la conversion

Les sauvegardes pendant la conversion des noms de fichiers de l'IDB sont possibles, car la conversion s'effectue en arrière-plan, et Data Protector reste totalement opérationnel.

Si les données du client dans l'IDB sont converties pendant la sauvegarde de ce client, la sauvegarde est réalisée avec l'option `Pas de journalisation` (par conséquent, aucune information relative aux fichiers et répertoires sauvegardés n'est consignée dans l'IDB pour ce client et cette session).

Restauration pendant la conversion

La restauration *pendant* la conversion des noms de fichiers est possible. Toutefois, seules les restaurations d'objets entiers ou de sélections de répertoires/fichiers de systèmes non-Windows, composés de caractères ASCII 7 bits, sont fiables.

Si des fichiers ou des répertoires sélectionnés pour la restauration d'un client spécifique contiennent des caractères non-ASCII (et proviennent d'une plate-forme non Windows), attendez que la conversion IDB des données de ce client soit terminée. L'Agent de disque de ce client doit être mis à niveau avant la restauration.

Sauvegarde et restauration après la conversion de l'IDB

Une fois toute la base IDB convertie et tous les Agents de disque sur tous les clients de la cellule mis à niveau vers la version A.06.00, l'opération de sauvegarde et de restauration se déroule normalement.

Conversion de l'IDB dans un Gestionnaire de cellule sous UNIX

Introduction

Cette section s'applique aux Gestionnaires de cellule sous UNIX dont la cellule contient des clients Windows et qui font l'objet d'une mise à niveau à partir de Data Protector A.05.00 ou A.05.10. Si vous effectuez une mise à niveau à partir de A.05.50, aucune conversion n'est requise.

La conversion de l'IDB demande un certain temps, selon sa taille et la configuration de votre cellule ; toutefois, cela n'affecte pas la réussite de vos opérations de sauvegarde ou de restauration. La conversion est réalisée en arrière-plan pendant les sauvegardes des clients Windows de la cellule, pendant une période spécifique. Après une sauvegarde complète de tous les objets sauvegarde de systèmes de fichiers de l'ensemble des clients Windows de la cellule, la conversion IDB est terminée et ne doit pas être effectuée à nouveau.

Par défaut, la conversion des noms de fichier dans l'IDB pendant les sauvegardes s'exécute pendant un mois, cette durée étant définie par l'option globale `ConvertFilenamesInIDBDuringBackup`. Pour plus de détails sur la modification du fichier d'options globales, consultez le *Guide de dépannage HP OpenView Storage Data Protector*.

Impact sur les performances

La conversion des noms de fichiers de l'IDB a un impact sur les performances. Pendant la conversion (l'option globale `ConvertFilenamesInIDBDuringBackup` est activée), une sauvegarde d'un client Windows est ralentie jusqu'à ce que la première sauvegarde complète du client soit réalisée. Reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage Data Protector* pour obtenir des informations détaillées.

Limites

Tenez compte des limites suivantes :

- Il est possible qu'un fichier, sauvegardé avec la version précédente de Data Protector et stocké dans l'IDB à l'aide de l'ancien codage, ait été supprimé du client avant la conversion de l'IDB. Dans ce cas, le nom de fichier n'est pas converti dans l'IDB. La même situation se produit si aucune sauvegarde n'a été effectuée au cours de la période de conversion (définie par l'option globale `ConvertFilenamesInIDBDuringBackup`). Cela rend la restauration d'un tel fichier plus difficile si des caractères non-ASCII sont utilisés dans le nom de fichier. Pour régler ce problème, reportez-vous au *Guide de dépannage HP OpenView Storage Data Protector*.
- Pour connaître les autres restrictions, reportez-vous au tableau 4-2 à la page 284.

Mise à niveau à partir de l'Edition serveur unique

La mise à niveau peut être effectuée à partir des versions suivantes :

- Des versions antérieures de l'Edition serveur unique (SSE) vers Data Protector A.06.00 Edition serveur unique. Pour plus de détails, reportez-vous à la section “Mise à niveau des versions antérieures de SSE vers Data Protector A.06.00 SSE” à la page 291.
- De Data Protector A.06.00 Edition serveur unique vers Data Protector A.06.00. Pour plus de détails, reportez-vous à la section “Mise à niveau de Data Protector A.06.00 SSE vers Data Protector A.06.00” à la page 291.

Mise à niveau des versions antérieures de SSE vers Data Protector A.06.00 SSE

La procédure de mise à niveau des versions antérieures de SSE vers Data Protector A.06.00 SSE est identique à celle des versions précédentes de Data Protector vers Data Protector A.06.00. Pour plus d'informations, reportez-vous à la section “Mise à niveau à partir de Data Protector A.05.x” à la page 253.

Mise à niveau de Data Protector A.06.00 SSE vers Data Protector A.06.00

Licences

Vous devez disposer d'une licence pour effectuer la mise à niveau de Data Protector A.06.00 Edition serveur unique vers Data Protector A.06.00. Pour plus de détails sur la gestion des licences, reportez-vous au Chapitre 5, “Attribution de licences Data Protector,” page 315.

La mise à niveau de l'Edition serveur unique de Data Protector A.06.00 vers Data Protector A.06.00 est proposée dans les deux cas de figure suivants :

- L'Edition serveur unique Data Protector est installée sur un système (Gestionnaire de cellule) uniquement. Reportez-vous à la section “Mise à niveau du Gestionnaire de cellule” à la page 292.

- L'Edition serveur unique Data Protector est installée sur plusieurs systèmes et vous souhaitez fusionner ces cellules. Reportez-vous à la section “Mise à niveau de plusieurs installations” à la page 292.

REMARQUE

Si vous souhaitez effectuer la mise à niveau d'une version précédente de l'Edition serveur unique vers une installation complète de Data Protector, commencez par mettre à niveau votre Edition serveur unique avec l'installation complète du même niveau de version. Ensuite, pour mettre à niveau cette installation complète vers Data Protector A.06.00, reportez-vous à la section “Mise à niveau à partir de Data Protector A.05.x” à la page 253.

Mise à niveau du Gestionnaire de cellule

Pour mettre à niveau le Gestionnaire de cellule Edition serveur unique, procédez comme suit :

1. Supprimez la licence Edition serveur unique :
   - Sous Windows :
     ```
     del
     <répertoire_Data_Protector>\Config\server\Cell\lic.dat
     ```
   - Sous UNIX :
     ```
     rm /etc/opt/omni/server/cell/lic.dat
     ```
2. Démarrez l'interface graphique utilisateur de Data Protector et ajoutez un mot de passe permanent.

Mise à niveau de plusieurs installations

Pour mettre à niveau l'Edition serveur unique Data Protector installée sur plusieurs systèmes, procédez comme suit :

1. Désignez parmi les systèmes où l'Edition serveur unique est installée celui qui doit devenir le nouveau Gestionnaire de cellule. Reportez-vous à la section “Choix du système Gestionnaire de cellule” à la page 11.

2. Mettez à niveau le Gestionnaire de cellule sélectionné comme suit :

   a. Supprimez la licence Edition serveur unique :

   `del` *`<répertoire_Data_Protector>`*`\Config\server\Cell\lic.dat` (sur les systèmes Windows) ou

   `rm /etc/opt/omni/server/cell/lic.dat` (sur les systèmes UNIX)

   b. Démarrez l'interface graphique utilisateur de Data Protector et ajoutez un mot de passe permanent.

3. Dans l'interface graphique, importez comme clients les autres systèmes Edition serveur unique dans le système Gestionnaire de cellule nouvellement créé.

4. Désinstallez l'Edition serveur unique Data Protector des autres systèmes. Reportez-vous à la section “Désinstallation du logiciel Data Protector” à la page 228.

5. Si nécessaire, importez les supports vers le nouveau Gestionnaire de cellule.

   Réalisez cette étape si vous envisagez de fréquentes restaurations à partir des supports créés sur les autres systèmes Edition serveur unique. Si ces restaurations sont peu probables, vous pouvez utiliser l'option `Lister depuis support`. Dans l'index de l'aide en ligne, recherchez : “importation, supports” pour obtenir des informations sur l'importation de supports et sur la restauration à l'aide de l'option `Lister depuis support`.

Mise à niveau de Windows NT vers une nouvelle version de Windows

Si votre Gestionnaire de cellule est installé sur un système Windows NT, vous devez mettre à niveau le système d'exploitation vers une nouvelle version car Windows NT n'est pas pris en charge par Data Protector A.06.00 en tant que plate-forme de Gestionnaire de cellule.

Si vous souhaitez mettre à niveau votre système d'exploitation de Windows NT vers une nouvelle version de Windows, vous devez prendre en compte l'impact de cette mise à niveau sur Data Protector.

Si le Gestionnaire de cellule Data Protector A.05.00 ou A.05.10 est installé sous Windows NT, et si vous souhaitez le mettre à niveau vers Data Protector A.06.00, procédez comme suit :

1. Mettez à niveau le système d'exploitation de Windows NT vers la nouvelle version de Windows. Pour plus d'informations, reportez-vous à la documentation Windows.
2. Mettez à niveau le Gestionnaire de cellule Data Protector A.05.00 ou A.05.10 vers Data Protector A.06.00. Pour connaître la procédure à suivre, reportez-vous à la section “Mise à niveau à partir de Data Protector A.05.x” à la page 253.

Mise à niveau de Solaris 7/8 vers Solaris 9

Si l'Agent de disque (DA) Data Protector A.06.00 est installé sous Solaris 7/8 et si vous voulez mettre à niveau le système d'exploitation vers Solaris 9, prenez en compte l'impact de cette mise à niveau sur Data Protector. Il est recommandé de remplacer l'Agent de disque générique Solaris installé sur le système par l'Agent de disque Solaris 9 pour garantir le bon fonctionnement de Data Protector et activer les options de sauvegarde avancées pour Solaris 9, comme par exemple la sauvegarde d'attributs étendus.

Réalisez la mise à niveau comme suit :

1. Mettez à niveau le système d'exploitation de Solaris 7/8 vers Solaris 9. Pour plus d'informations, reportez-vous à la documentation Solaris.
2. Installez l'Agent de disque à distance sur le système mis à niveau à l'aide d'un Serveur d'installation. L'Agent de disque générique Solaris sera ainsi remplacé par l'Agent de disque Solaris 9. Reportez-vous à la section “Installation distante de clients Data Protector” à la page 54 ou à la page man de `ob2install`.

Migration de HP-UX 11.x vers HP-UX 11.23

Cette section décrit la procédure à suivre pour faire migrer votre Gestionnaire de cellule d'un système HP-UX 11.x basé sur une architecture PA-RISC vers un système HP-UX 11.23 pour l'architecture Intel Itanium 2 (IA-64).

Limites

Pour plus d'informations sur les versions des systèmes d'exploitation, les plates-formes, les processeurs et les éléments Data Protector pris en charge et pour connaître les correctifs requis, les limites générales et les conditions requises pour l'installation, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

- La migration est uniquement prise en charge à partir du Gestionnaire de cellule Data Protector A.06.00 sur un système HP-UX 11.x basé sur PA-RISC.
- Pour connaître les combinaisons de configurations MoM prises en charge, reportez-vous à la section “Informations spécifiques à MoM” à la page 300.

Recommandation

- Il est recommandé de convertir les noms de fichier dans la base IDB avant la migration. Reportez-vous à la section “Conversion des noms de fichiers de la base de données IDB” à la page 281.

Licences

Le nouveau Gestionnaire de cellule (système IA-64) aura une adresse IP différente de celle de l'ancien Gestionnaire de cellule ; par conséquent, vous devriez demander la migration des licences avant de procéder à la migration du système. Pendant une période limitée, les licences des deux systèmes seront opérationnelles. Si les licences sont basées sur une plage IP et si l'adresse IP du nouveau Gestionnaire de cellule se situe dans cette plage, aucune reconfiguration de licence n'est nécessaire. Pour plus de détails, reportez-vous à la section “Migration de licence vers Data Protector A.06.00” à la page A-21.

NOTE

L'interface utilisateur n'est pas prise en charge sur HP-UX 11.23. Toutefois, vous pouvez utiliser la commande `omniusers` pour créer un compte utilisateur distant sur le nouveau Gestionnaire de cellule. Vous pouvez alors utiliser ce compte utilisateur avec l'interface graphique

utilisateur de Data Protector installée pour lancer l'interface et vous connecter au nouveau Gestionnaire de cellule. Reportez-vous à la page `omniusers` du manuel.

Procédure de migration

Réalisez la procédure de migration comme suit :

1. Installez un client Data Protector sur le système IA-64 et importez-le dans la cellule de l'ancien Gestionnaire de cellule. Si vous avez l'intention de configurer Data Protector dans un cluster, installez le client sur le noeud principal. Reportez-vous à la section “Installation de clients HP-UX” à la page 74.
2. Exécutez la commande suivante sur l'*ancien* Gestionnaire de cellule pour ajouter le nom d'hôte du système IA-64 à la liste des hôtes approuvés sur les clients sécurisés :

   `omnimigrate.pl -prepare_clients` *<Nom_nouveau_GC>*, où *<Nom_nouveau_GC>* correspond au nom de client du système IA-64 de l'étape précédente.

   Pour plus d'informations sur les groupes d'hôtes approuvés et la sécurisation des clients Data Protector, reportez-vous aux sections “Sécurisation des clients” à la page 210 et “Groupement d'hôtes approuvés” à la page 222.
3. Sauvegardez la base de données IDB. Reportez-vous au mot clé “Sauvegarde IDB” dans l'index de l'aide en ligne.
4. Restaurez la base IDB dans un emplacement temporaire sur le système IA-64. Reportez-vous au mot clé “Restauration IDB” dans l'index de l'aide en ligne.
5. Désinstallez le client Data Protector du nouveau système IA-64. Reportez-vous à la section “Désinstallation d'un client Data Protector” à la page 229.
6. Installez le Gestionnaire de cellule Data Protector sur le système IA-64. Si vous avez l'intention de configurer Data Protector dans un cluster, installez le Gestionnaire de cellule sur le noeud principal en tant que Gestionnaire de cellule *autonome* (non compatible avec les clusters). Reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector” à la page 19.
7. Si vous avez modifié le port Inet Data Protector par défaut sur

l'ancien Gestionnaire de cellule, définissez le même port Inet sur le nouveau Gestionnaire de cellule. Reportez-vous à la section “Modification du numéro de port par défaut” à la page 30.

8. Déplacez la base de données IDB restaurée (résidant dans un emplacement temporaire sur le nouveau Gestionnaire de cellule) et les données de configuration dans le même emplacement sur le nouveau Gestionnaire de cellule que celui qu'elles occupaient sur l'ancien Gestionnaire de cellule. Reportez-vous au mot clé “Restauration IDB” dans l'index de l'aide en ligne.

   Si l'ancien Gestionnaire de cellule était compatible avec les clusters, commentez les variables `SHARED_DISK_ROOT` et `CS_SERVICE_HOSTNAME` dans le fichier `/etc/opt/omni/server/sg/sg.conf`. Cela est nécessaire même si le nouveau Gestionnaire de cellule est compatible avec les clusters.

9. Pour faire migrer l'IDB et les clients vers le nouveau Gestionnaire de cellule et pour reconfigurer les paramètres du Gestionnaire de cellule, procédez comme suit sur le *nouveau* Gestionnaire de cellule :

   - Si vous souhaitez configurer un Gestionnaire de cellule IA-64 autonome :

     a. Exécutez la commande `omnimigrate.pl -configure`. Reportez-vous à la page man `omnimigrate.pl`.

   - Si vous souhaitez configurer un Gestionnaire de cellule IA-64 compatible avec les clusters :

     a. Exécutez la commande `omnimigrate -configure_idb` pour configurer l'IDB de l'ancien Gestionnaire de cellule pour une utilisation avec le nouveau Gestionnaire de cellule. Reportez-vous à la page man `omnimigrate.pl`.

     b. Exécutez la commande `omnimigrate -configure_cm` pour reconfigurer les données de configuration de l'ancien Gestionnaire de cellule pour une utilisation avec le nouveau Gestionnaire de cellule. Reportez-vous à la page man `omnimigrate.pl`.

     c. Exportez l'ancien serveur virtuel de la cellule en exécutant la commande `omnicc -export_host` *<Nom_ancien_GC>*.

     d. Configurez le Gestionnaire de cellule principal et secondaire. Reportez-vous au mot clé “Configuration de l'intégration de MC/ServiceGuard” dans l'index de l'aide en ligne.

e. Exécutez la commande `omnimigrate -configure_clients` pour faire migrer les client de l'ancien Gestionnaire de cellule au nouveau Gestionnaire de cellule. Notez que l'ancien Gestionnaire de cellule conserve les clients dans les fichiers de configuration, mais il ne sera plus leur Gestionnaire de cellule.

REMARQUE Si le répertoire `/etc/opt/omni/server` est situé sur le volume de cluster partagé, les changements de configuration effectués par le script `omnimigrate.pl` affecteront tous les noeuds du cluster.

REMARQUE L'ancien Gestionnaire de cellule deviendra automatiquement un client dans la nouvelle cellule. Vous pouvez désinstaller le composant Gestionnaire de cellule de l'ancien Gestionnaire de cellule car il n'est plus nécessaire. Reportez-vous à la section “Changement de composants logiciels Data Protector” à la page 242.

10. Configurez les licences sur le nouveau Gestionnaire de cellule. Reportez-vous à la section “Structure de produit et licences Data Protector A.06.00” à la page A-2.
11. Créez un compte utilisateur distant sur le nouveau Gestionnaire de cellule et utilisez-le sur n'importe quel autre système équipé de l'interface graphique utilisateur de Data Protector afin de lancer cette dernière et de vous connecter au Gestionnaire de cellule. Pour plus de détails, reportez-vous à la page `omniusers` du manuel.
12. Des étapes supplémentaires sont requises dans les situations suivantes :
    - Votre cellule fait partie d'un environnement MoM. Reportez-vous à la section “Informations spécifiques à MoM” à la page 300.
    - Votre cellule fonctionne de part et d'autre d'un pare-feu. Reconfigurez tous les paramètres liés au pare-feu sur le nouveau Gestionnaire de cellule. Reportez-vous au mot clé “Environnements pare-feu” dans l'index de l'aide en ligne.
    - Vous souhaitez disposer d'un Serveur d’installation sur votre nouveau Gestionnaire de cellule. Reportez-vous à la section “Détails relatifs au Serveur d’installation” à la page 301.

Informations spécifiques à MoM

Si le nouveau Gestionnaire de cellule doit être configuré dans le MoM, des étapes supplémentaires sont requises une fois la procédure de migration de base terminée. Les étapes requises dépendent de la configuration du MoM pour l'ancien et le nouveau Gestionnaire de cellule dans votre environnement. Les combinaisons prises en charge sont les suivantes :

- L'ancien Gestionnaire de cellule était un client MoM ; le nouveau Gestionnaire de cellule sera un client MoM du même Gestionnaire MoM.

  Effectuez les opérations suivantes :

  1. Dans le Gestionnaire MoM, exportez l'ancien Gestionnaire de cellule de la cellule du Gestionnaire MoM et importez le nouveau Gestionnaire de cellule. Reportez-vous au mot clé “Exportation de systèmes client” dans l'index de l'aide en ligne.
  2. Ajoutez l'administrateur MoM à la liste des utilisateurs sur le nouveau Gestionnaire de cellule. Reportez-vous au mot clé “Administrateur MoM, ajout”, dans l'index de l'aide en ligne.

- L'ancien Gestionnaire de cellule était un Gestionnaire MoM ; le nouveau Gestionnaire de cellule sera un Gestionnaire MoM.

  Si l'ancien Gestionnaire MoM était le seul client sur le MoM, aucune action n'est nécessaire. Dans le cas contraire, effectuez les opérations suivantes :

  1. Dans l'ancien Gestionnaire MoM (l'ancien Gestionnaire de cellule), exportez tous les clients MoM.
  2. Dans le nouveau Gestionnaire MoM (le nouveau Gestionnaire de cellule), importez tous les clients MoM.
  3. Ajoutez l'administrateur MoM à la liste des utilisateurs sur tous les nouveaux clients MoM.

REMARQUE

L'interface utilisateur n'est pas prise en charge sur HP-UX 11.23. Toutefois, vous pouvez utiliser la commande `omniusers` pour créer un compte utilisateur distant sur le nouveau Gestionnaire de cellule. Vous pouvez alors utiliser ce compte utilisateur sur n'importe quel système

équipé de l'interface graphique utilisateur de Data Protector pour lancer l'interface MoM et vous connecter au nouveau Gestionnaire de cellule. Reportez-vous à la page `omniusers` du manuel.

Détails relatifs au Serveur d’installation

La migration du Serveur d’installation ne s'effectue pas dans le cadre de la migration du Gestionnaire de cellule. Si un Serveur d’installation est installé sur votre ancien Gestionnaire de cellule, il ne migrera pas vers le nouveau Gestionnaire de cellule et restera le Serveur d’installation de votre cellule.

Si vous souhaitez également utiliser le nouveau Gestionnaire de cellule en tant que Serveur d’installation, installez le composant Serveur d’installation sur le nouveau Gestionnaire de cellule après la migration et importez-le dans la cellule. Reportez-vous au mot clé "Serveur d’installation" dans l'index de l'aide en ligne.

Migration d'un système Windows 32 bits vers un système Windows 64 bits

Cette section décrit la procédure de migration du Gestionnaire de cellule existant d'un système Windows 32 bits vers un système Windows 64 bits.

Limites

Pour plus d'informations sur les versions des systèmes d'exploitation, les plates-formes, les processeurs et les éléments Data Protector pris en charge et pour connaître les correctifs requis, les limites générales et les conditions requises pour l'installation, reportez-vous aux *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

Condition préalable

- Avant la migration, le Gestionnaire de cellule de Data Protector sur un système Windows 32 bits doit être mis à niveau vers Data Protector A.06.00.

Recommandation

- Dans le cas d'une mise à niveau à partir de Data Protector A.05.10 ou d'une version précédente, nous vous recommandons d'effectuer la conversion des noms de fichiers dans l'IDB avant la migration. Reportez-vous à la section “Conversion des noms de fichiers de la base de données IDB” à la page 281.

Licences

Le nouveau Gestionnaire de cellule aura une adresse IP différente de celle de l'ancien Gestionnaire de cellule ; par conséquent, vous devriez demander la migration des licences avant de procéder à la migration du système. Pendant une période limitée, les licences des deux systèmes seront opérationnelles. Si les licences sont basées sur une plage IP et si l'adresse IP du nouveau Gestionnaire de cellule se situe dans cette plage, aucune reconfiguration de licence n'est nécessaire. Reportez-vous à la section “Migration de licence vers Data Protector A.06.00” à la page A-21 pour plus de détails.

Procédure de migration

Réalisez la migration comme suit :

1. Installez un client Data Protector sur le système 64 bits et importez-le dans la cellule de l'ancien Gestionnaire de cellule. Reportez-vous à la section “Installation de clients Windows” à la page 68.

2. Sur l'*ancien* Gestionnaire de cellule, ajoutez le nom d'hôte du système 64 bits à la liste des hôtes approuvés sur les clients sécurisés. Dans le répertoire *<répertoire_Data_Protector>*\bin, exécutez :

   ```
   perl.exe winomnimigrate.pl -prepare_clients
   <Nom_nouveau_gestionnaire>
   ```

   Pour plus d'informations sur les hôtes approuvés et la sécurisation des clients Data Protector, reportez-vous aux sections “Sécurisation des clients” à la page 210 et “Groupement d'hôtes approuvés” à la page 222.

3. Sauvegardez la base de données IDB. Dans l'index de l'aide en ligne, recherchez : "sauvegarde de la base de données interne".

4. Restaurez la base IDB dans un emplacement temporaire sur le système 64 bits. Dans l'index de l'aide en ligne, recherchez : "restauration de la base de données interne".

5. Désinstallez le client Data Protector du système 64 bits. Reportez-vous à la section “Désinstallation d'un client Data Protector” à la page 229.

6. Installez le Gestionnaire de cellule Data Protector sur le système 64 bits. Reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d’installation (IS) de Data Protector” à la page 19.

7. Si vous avez modifié le port Inet Data Protector par défaut sur l'ancien Gestionnaire de cellule, définissez le même port Inet sur le nouveau Gestionnaire de cellule. Reportez-vous à la section “Modification du numéro de port par défaut” à la page 30.

8. Déplacez la base de données IDB restaurée (résidant dans un emplacement temporaire sur le nouveau Gestionnaire de cellule) et les données de configuration sur le nouveau Gestionnaire de cellule, dans le même emplacement qu'elles occupaient sur l'ancien Gestionnaire de cellule. Dans l'index de l'aide en ligne, recherchez : "restauration de la base de données interne".

9. Pour faire migrer l'IDB et les clients vers le nouveau Gestionnaire de cellule et pour reconfigurer les paramètres du Gestionnaire de cellule, procédez comme suit sur le *nouveau* Gestionnaire de cellule :

   - Configurez un Gestionnaire de cellule autonome. Dans le répertoire *<répertoire_Data_Protector>*\bin, exécutez :

     ```
     perl.exe winomnimigrate.pl -configure
     ```

- Pour configurer un Gestionnaire de cellule compatible cluster :

  a. Dans le répertoire *<répertoire_Data_Protector>*\bin, exécutez `perl.exe winomnimigrate.pl -configure_idb` afin de configurer la base de données IDB de l'ancien Gestionnaire de cellule en vue d'une utilisation sur le nouveau Gestionnaire de cellule.

  b. Dans le répertoire *<répertoire_Data_Protector>*\bin, exécutez `perl.exe winomnimigrate.pl -configure_cm` afin de reconfigurer les données de configuration transférées de l'ancien Gestionnaire de cellule en vue d'une utilisation sur le nouveau Gestionnaire de cellule.

  c. Exportez l'ancien serveur virtuel de la cellule en exécutant la commande `omnicc -export_host` *<Nom_ancien_gestionnaire>*.

  d. Dans le répertoire *<répertoire_Data_Protector>*\bin, exécutez `perl.exe winomnimigrate.pl -configure_clients` pour faire migrer les clients de l'ancien Gestionnaire de cellule vers le nouveau Gestionnaire de cellule. Notez que l'ancien Gestionnaire de cellule conserve les clients dans les fichiers de configuration, mais il ne sera plus leur Gestionnaire de cellule.

REMARQUE

L'ancien Gestionnaire de cellule deviendra automatiquement un client dans la nouvelle cellule. Vous pouvez désinstaller le composant Gestionnaire de cellule de l'ancien Gestionnaire de cellule car il n'est plus nécessaire. Reportez-vous à la section “Changement de composants logiciels Data Protector” à la page 242.

10. Configurez les licences sur le nouveau Gestionnaire de cellule. Reportez-vous à la section “Structure de produit et licences Data Protector A.06.00” à la page A-2.
11. Des étapes supplémentaires sont nécessaires dans les cas suivants :

    - Votre cellule fait partie de l'environnement MoM. Reportez-vous à la section “Informations spécifiques à MoM” à la page 305.

- Votre cellule fonctionne de part et d'autre d'un pare-feu. Reconfigurez tous les paramètres liés au pare-feu sur le nouveau Gestionnaire de cellule. Dans l'index de l'aide en ligne, recherchez : "environnements pare-feu".
- Vous souhaitez disposer d'un Serveur d'installation sur votre nouveau Gestionnaire de cellule. Reportez-vous à la section “Détails relatifs au Serveur d'installation” à la page 306.

Informations spécifiques à MoM

Si le nouveau Gestionnaire de cellule doit être configuré dans le MoM, des étapes supplémentaires sont requises une fois la procédure de migration de base terminée. Les étapes requises dépendent de la configuration du MoM pour l'ancien et le nouveau Gestionnaire de cellule dans votre environnement. Les combinaisons prises en charge sont les suivantes :

- L'ancien Gestionnaire de cellule était un client MoM ; le nouveau Gestionnaire de cellule sera un client MoM du même Gestionnaire MoM.

  Effectuez les opérations suivantes :

  1. Dans le Gestionnaire MoM, exportez l'ancien Gestionnaire de cellule de la cellule du Gestionnaire MoM et importez le nouveau Gestionnaire de cellule. Dans l'index de l'aide en ligne, recherchez : "systèmes clients, exportation".
  2. Ajoutez l'administrateur MoM à la liste des utilisateurs sur le nouveau Gestionnaire de cellule. Dans l'index de l'aide en ligne, recherchez : "administrateur MoM, ajout".

- L'ancien Gestionnaire de cellule était un Gestionnaire MoM ; le nouveau Gestionnaire de cellule sera un Gestionnaire MoM.

  Si l'ancien Gestionnaire MoM était le seul client sur le MoM, aucune action n'est nécessaire. Dans le cas contraire, effectuez les opérations suivantes :

  1. Dans l'ancien Gestionnaire MoM (l'ancien Gestionnaire de cellule), exportez tous les clients MoM.
  2. Dans le nouveau Gestionnaire MoM (le nouveau Gestionnaire de cellule), importez tous les clients MoM.

3. Ajoutez l'administrateur MoM à la liste des utilisateurs sur tous les clients MoM.

Détails relatifs au Serveur d’installation

La migration du Serveur d’installation ne s'effectue pas dans le cadre de la migration du Gestionnaire de cellule. Si un Serveur d’installation est installé sur votre ancien Gestionnaire de cellule, il ne fera pas l'objet d'une migration vers le nouveau Gestionnaire de cellule.

Si vous souhaitez également utiliser le nouveau Gestionnaire de cellule en tant que Serveur d’installation, installez le composant Serveur d’installation sur le nouveau Gestionnaire de cellule après la migration et importez-le dans la cellule. Dans l'index de l'aide en ligne, recherchez : “Serveur d’installation”.

Mise à niveau du Gestionnaire de cellule configuré sur MC/ServiceGuard

Lors d'une mise à niveau, seule la base de données est mise à niveau : l'ancienne version du produit est supprimée. Data Protector A.06.00 est installé avec la sélection d'agents par défaut et les autres agents sont supprimés. Pour obtenir une configuration dont l'état est équivalent à l'état antérieur à la mise à niveau, vous devez sélectionner manuellement les autres agents souhaités pendant la procédure de mise à niveau, ou les réinstaller ensuite sur chacun des nœuds physiques.

La procédure de mise à niveau de Data Protector A.05.00, Data Protector A.05.10 ou Data Protector A.05.50 consiste à mettre à niveau le nœud principal et les nœuds secondaires. Pour cela, procédez comme suit :

Nœud principal

Connectez-vous au nœud principal et procédez comme suit :

1. Arrêtez l'ancien package OmniBack II/Data Protector en exécutant la commande `cmhaltpkg <nom_pkg>` (où `<nom_pkg>` correspond au nom du package de clusters). Par exemple :

   ```
   cmhaltpkg ob2cl
   ```

2. Activez le groupe de volumes en mode exclusif :

   ```
   vgchange -a e -q y <nom_gv>
   ```

   Par exemple :

   ```
   vgchange -a e -q y /dev/vg_ob2cm
   ```

3. Montez le volume logique sur le disque partagé :

   ```
   mount <chemin_vl> <disque_partagé>
   ```

   Le paramètre `<chemin_vl>` correspond au nom de chemin du volume logique et le paramètre `<disque_partagé>` au point de montage ou répertoire partagé. Par exemple :

   ```
   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
   ```

4. Mettez à niveau le Gestionnaire de cellule en suivant la procédure décrite dans les paragraphes qui suivent. Notez que certaines étapes sont différentes selon la version du produit que vous mettez à niveau

vers Data Protector A.06.00. Reportez-vous à la section “Mise à niveau du Gestionnaire de cellule et du Serveur d’installation UNIX” à la page 253.

5. Arrêtez les services Data Protector s'ils sont en cours d'exécution :

   ```
   /opt/omni/sbin/omnisv -stop
   ```

6. Démontez le disque partagé :

   ```
   umount <disque_partagé>
   ```

   Par exemple :

   ```
   umount /omni_shared
   ```

7. Désactivez le groupe de volumes :

   ```
   vgchange -a n <nom_gv>
   ```

   Par exemple :

   ```
   vgchange -a n /dev/vg_ob2cm
   ```

Nœud secondaire

Connectez-vous au nœud secondaire et procédez comme suit :

1. Activez le groupe de volumes en mode exclusif :

   ```
   vgchange -a e -q y <nom_gv>
   ```

2. Montez le volume logique sur le disque partagé :

   ```
   mount <chemin_vl> <disque_partagé>
   ```

3. Mettez à niveau le Gestionnaire de cellule. Les étapes sont différentes selon la version du produit que vous mettez à niveau vers Data Protector A.06.00. Suivez les étapes de la procédure décrite dans le chapitre “Mise à niveau du Gestionnaire de cellule et du Serveur d’installation UNIX” à la page 253.

4. Renommez les scripts de démarrage `csfailover.sh` et `mafailover.ksh` dans le répertoire `/etc/opt/omni/server/sg` (en leur donnant par exemple les noms `csfailover_DP51.sh` et `mafailover_DP51.ksh`) et copiez les nouveaux scripts `csfailover.sh` et `mafailover.ksh` du répertoire `/opt/omni/newconfig/etc/opt/omni/server/sg` vers le répertoire `/etc/opt/omni/server/sg`.

   Si vous avez personnalisé vos anciens scripts de démarrage, implémentez à nouveau les modifications dans les nouveaux scripts de démarrage.

REMARQUE Les chemins par défaut de certains fichiers de configuration, fichiers journaux et de base de données (sous UNIX) ont été modifiés dans Data Protector A.06.00. Certains fichiers figurant dans les répertoires server et client sont désormais divisés. Reportez-vous à la section “Fichiers de configuration sous UNIX” à la page B-85.

5. Arrêtez les services Data Protector s'ils sont en cours d'exécution :

   ```
   /opt/omni/sbin/omnisv -stop
   ```

6. Démontez le disque partagé :

   ```
   umount <disque_partagé>
   ```

7. Désactivez le groupe de volumes :

   ```
   vgchange -a n <nom_gv>
   ```

Nœud principal Reconnectez-vous au nœud principal et procédez comme suit :

1. Arrêtez le package Data Protector :

   ```
   cmrunpkg <nom_pkg>
   ```

   Assurez-vous que le basculement du package et les options de basculement des nœuds sont activés.

2. Configurez le Gestionnaire de cellule. Veillez à ne pas vous placer dans les répertoires `/etc/opt/omni` ou `/var/opt/omni` ou dans leurs sous-répertoires lorsque vous exécutez ce script. Assurez-vous également qu'il n'existe aucun sous-répertoire monté dans `/etc/opt/omni` ou `/var/opt/omni`. Exécutez :

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

3. Réimportez l'hôte virtuel :

   ```
   omnicc -import_host <nom_hôte_virtuel> -virtual
   ```

4. Changez le nom du Gestionnaire de cellule dans la base de données IDB :

   ```
   omnidbutil -change_cell_name
   ```

5. Si le Serveur d'installation se trouve dans le même package que le Gestionnaire de cellule, importez le nom d'hôte virtuel du Serveur d'installation :

   ```
   omnicc -import_is <nom_hôte_virtuel>
   ```

REMARQUE

Toutes les demandes provenant des Gestionnaires de cellule sont enregistrées dans le fichier `/var/opt/omni/log/inet.log` sur les clients. Pour empêcher l'écriture d'entrées inutiles dans le journal, sécurisez les clients. Pour plus d'informations sur la procédure de sécurisation d'une cellule, reportez-vous à la section “Considérations sur la sécurité” à la page 207.

Mise à niveau du Gestionnaire de cellule configuré sur Microsoft Cluster Server

La mise à niveau du Gestionnaire de cellule Data Protector A.05.00, A.05.10 ou A.05.50 vers Data Protector A.06.00 sur Microsoft Cluster Server (MSCS) se fait en local, à partir du DVD-ROM d'installation de Windows.

REMARQUE Il est recommandé d'installer MSI 2.0 sur tous les noeuds de clusters.

Pour effectuer la mise à niveau, procédez comme suit :

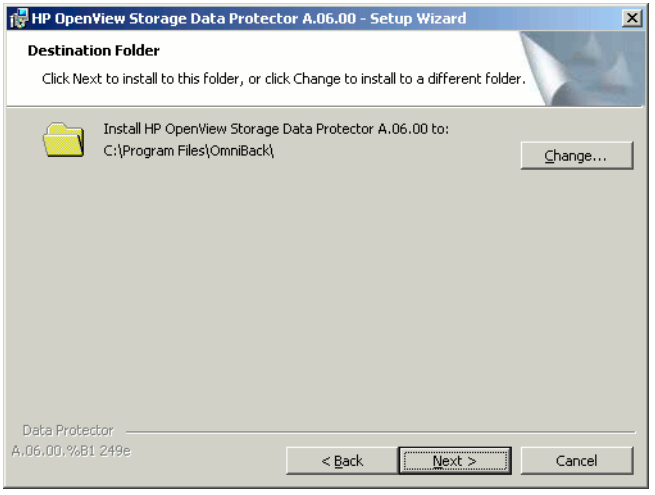
1. Insérez le DVD-ROM d'installation Windows et exécutez `\Windows_other\i386\setup.exe`. Il est recommandé de lancer l'installation sur le noeud de serveur virtuel actuellement actif.

   Le programme d'installation détecte automatiquement l'ancienne version du produit et vous invite à la mettre à niveau vers Data Protector A.06.00.

   Cliquez sur `Suivant` pour continuer.

2. Data Protector sélectionne automatiquement les composants qui ont été installés.

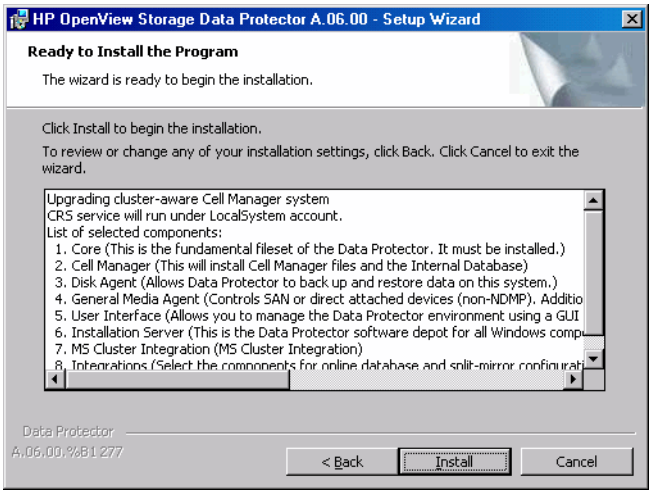
Figure 4-5 Sélection des composants



3. La liste récapitulative des composants sélectionnés s'affiche. Cliquez sur `Installer` pour effectuer la mise à niveau.

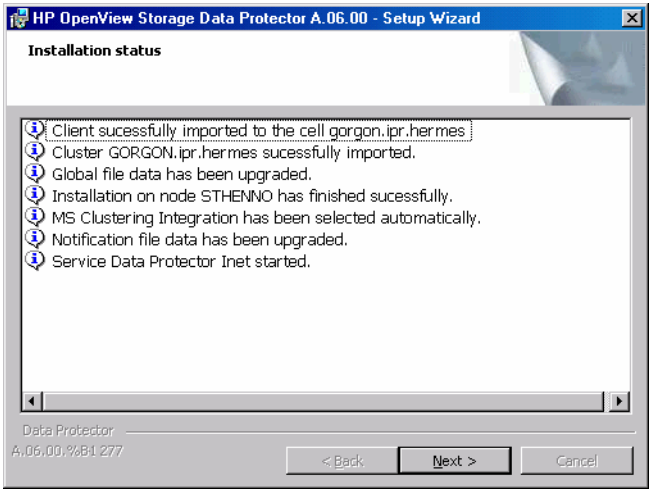
   Notez qu'à l'issue de la mise à niveau, tous les nœuds disposent du même jeu de composants.

Figure 4-6 Page de résumé des composants sélectionnés



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

Figure 4-7 Page d'état de l'installation



5. Si des clients UNIX sont présents dans la cellule, la page `Conversion de l'IDB` s'affiche. Reportez-vous à la section

"Conversion des noms de fichiers de la base de données IDB" à la page 281.

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

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

   Il *n'*est *pas* recommandé d'installer l'utilitaire HP OpenView AutoPass sur Microsoft Cluster, car il ne serait installé que sur un seul nœud et non sur tous. Toutefois, si vous installez AutoPass, vous devez désinstaller Data Protector du même noeud sur lequel il était installé, une fois que vous décidez de supprimer Data Protector du système.

   Cliquez sur `Terminer`.

REMARQUE Si vous mettez à niveau des clients compatibles cluster, commencez par mettre à niveau séparément chaque cluster, puis réimportez le serveur virtuel. La mise à niveau à distance n'est pas prise en charge.

5 Attribution de licences Data Protector

Description du chapitre

Ce chapitre contient des informations sur la vérification et le signalement des licences Data Protector ainsi que sur l'obtention et l'installation de mots de passe Data Protector.

Introduction

La structure de Data Protector A.06.00 et son système d'attribution de licences comprennent trois catégories principales :

1. Packs Starter
2. Extensions de lecteur et extensions de bibliothèque
3. Extensions fonctionnelles

REMARQUE Les licences UNIX du produit fonctionnent sur toutes les plates-formes, avec le même niveau de fonctionnalité quelle que soit la plate-forme, tandis que les licences Windows fonctionnent uniquement sur les plates-formes Windows, NetWare et Linux.

Liés au Gestionnaire de cellule, les mots de passe sont valides pour l'intégralité de la cellule Data Protector. Les clients ne requièrent aucune licence pour les sauvegardes de système de fichiers ou d'image disque.

Vérification et signalement des licences manquantes

La présence des licences Data Protector est vérifiée et leur absence éventuelle est signalée lors de diverses opérations de Data Protector, par exemple :

- Dans le cadre du mécanisme de vérification et de maintenance de Data Protector, la présence des licences est vérifiée et leur absence éventuelle est consignée dans le journal d'événements de Data Protector. Le journal d'événements de Data Protector se trouve sur le Gestionnaire de cellule dans *<répertoire_Data_Protector>*\log\server\Ob2EventLog.txt. Pour plus d'informations sur le mécanisme de vérification et de maintenance de Data Protector, recherchez l'entrée suivante dans l'index de l'aide en ligne : "journal d'événements, Data Protector".
- Si des licences manquantes sont signalées dans le journal des événements de Data Protector au démarrage de l'interface utilisateur de Data Protector, une notification du journal des événements s'affiche. Pour plus d'informations sur le journal d'événements de Data Protector, recherchez l'entrée suivante dans l'index de l'aide en ligne : "journal d'événements, Data Protector".
- Au démarrage d'une session Data Protector, la présence des licences est vérifiée et leur absence éventuelle est signalée.

Les licences Data Protector sont regroupées comme suit selon leurs caractéristiques :

- Licences liées au Gestionnaire de cellule
- Licences basées sur les entités
- Licences basées sur la capacité

Licences liées au Gestionnaire de cellule

Les licences liées au Gestionnaire de cellule Data Protector sont les suivantes :

- Packs Starter
- Extension Manager-of-Managers
- Edition serveur unique

Lorsqu'un composant Data Protector donné, tel que le Gestionnaire de cellule (inclus dans le Pack Starter) ou le Manager-of-Managers, est présent dans la cellule, seule la présence des licences de base et spéciales est vérifiée.

Licences basées sur les entités

Les licences Data Protector basées sur les entités sont les suivantes :

- Extension de bibliothèque pour une bibliothèque de 61 à 250 emplacements et pour une bibliothèque avec un nombre illimité d'emplacements
- Extension de lecteur pour UNIX / NAS / SAN et extension de lecteur pour Windows / NetWare / Linux (Intel)
- Extension pour sauvegarde en ligne d'un seul système UNIX et extension pour sauvegarde en ligne d'un seul système Windows / Linux

Lorsque l'un des éléments soumis aux licences basées sur la source est configuré dans la cellule, la présence et le nombre des licences requises basées sur les entités sont vérifiés.

Data Protector compare le nombre d'éléments configurés basés sur les entités et le nombre de licences basées sur les entités. S'il y a moins de licences que d'éléments configurés, Data Protector émet une notification.

Dans le cas des deux premières licences de la liste ci-dessus, il convient de respecter la règle suivante :

Lorsqu'un périphérique de sauvegarde est configuré dans un environnement SAN pour plusieurs clients Data Protector, la fonctionnalité multi-chemins doit être utilisée pour que Data Protector le reconnaisse comme un périphérique de sauvegarde unique.

Licences basées sur la capacité

Les licences Data Protector basées sur la capacité sont les suivantes :

- Sauvegarde avec temps d'indisponibilité nul (ZDB) pour HP StorageWorks XP pour 1 To et 10 To
- Sauvegarde avec temps d'indisponibilité nul pour HP StorageWorks Enterprise Virtual Array pour 1 To et 10 To
- Sauvegarde avec temps d'indisponibilité nul pour EMC Symmetrix pour 1 To et 10 To
- Restauration instantanée pour HP StorageWorks XP pour 1 To et 10 To
- Restauration instantanée pour HP StorageWorks Enterprise Virtual Array pour 1 To et 10 To
- Sauvegarde directe pour HP StorageWorks Disk Array XP pour 1 To et 10 To
- Sauvegarde directe pour HP StorageWorks Enterprise Virtual Array pour 1 To et 10 To
- Sauvegarde directe via NDMP pour 1 To et 10 To
- Sauvegarde avancée sur disque pour 1 To, 10 To et 100 To

La licence de sauvegarde avancée sur disque basée sur la capacité diffère des autres licences de ce groupe. Pour cela, reportez-vous à la section “Licence de sauvegarde avancée sur disque” à la page 322.

Lorsqu'une licence basée sur la capacité (autre que celle de sauvegarde avancée sur disque) est vérifiée, la quantité *totale* de l'espace disque des unités logiques sauvegardées est comparée au nombre de licences installées.

La vérification des licences est effectuée de façon à vous permettre de réaliser une restauration instantanée ou une sauvegarde même si vous avez atteint la capacité autorisée par la licence. Dans ce cas, un message d'avertissement apparaît au cours de la session de sauvegarde vous informant que vous avez dépassé la capacité autorisée par la licence.

La capacité de disque utilisée est calculée d'après les informations d'historique collectées au cours de chaque session de sauvegarde avec temps d'indisponibilité nul ou de sauvegarde directe. L'intervalle de temps retenu est vingt-quatre heures. Data Protector calcule la capacité

de disque utilisée en tenant compte des disques ayant été utilisés pendant toutes les sessions au cours des dernières vingt-quatre heures et compare la capacité ainsi obtenue à la capacité autorisée par la licence.

En cas de violation de licence, un message d'avertissement est émis au cours de la sauvegarde. En outre, l'outil de génération de rapports sur les licences est exécuté quotidiennement et il inscrit une notification dans le journal des événements de Data Protector en cas de dépassement de la capacité autorisée par la licence.

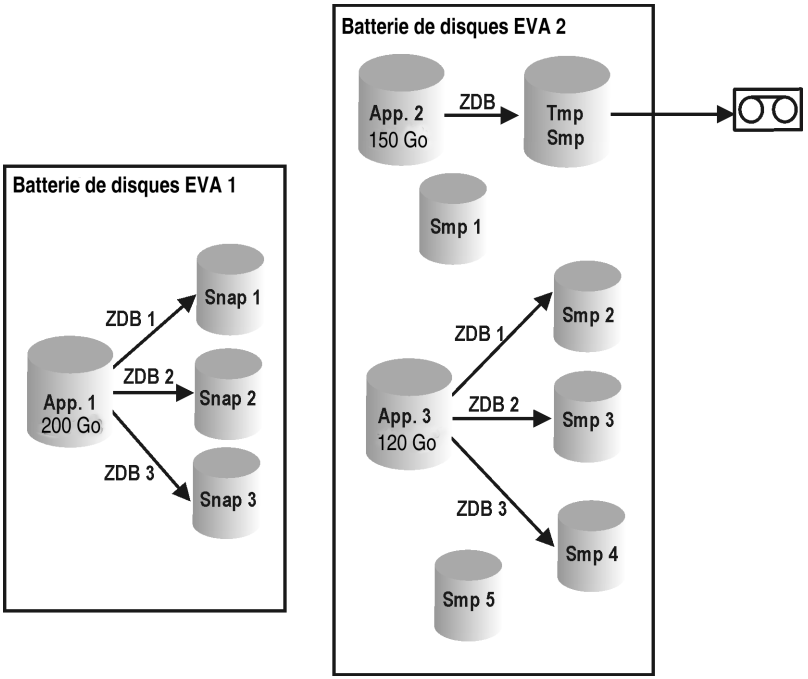
Calcul de la capacité utilisée

La fonction de calcul de la capacité utilisée évalue la capacité autorisée par la licence pour chaque type de baie de disques ayant été utilisé au cours des dernières vingt-quatre heures. Les disques utilisés deux fois ou plus au cours de l'intervalle de temps spécifié ne sont comptabilisés qu'une seule fois. Chaque baie de disques est identifiée par son numéro d'identification. L'utilisation des numéros d'identification des baies indique si une baie a déjà été comptabilisée.

Si une session de sauvegarde avec temps d'indisponibilité nul incluant une restauration instantanée ou une sauvegarde directe a été exécutée, la capacité totale de l'unité d'origine est calculée pour inclure d'une part la capacité utilisée pour la sauvegarde avec temps d'indisponibilité nul par baie de disques et d'autre part la capacité utilisée pour la restauration instantanée ou la sauvegarde directe par baie de disques.

Prenons l'exemple d'un scénario avec deux baies de disques EVA. Une baie contient un seul disque (serveur 1) d'une capacité de 200 Go utilisée pour la protection des données. Les sessions de sauvegarde déclenchées trois fois par jour incluent une option de restauration instantanée. Trois snapshots sont conservés simultanément ; ils sont utilisés tour à tour à des fins de restauration instantanée. La deuxième baie de disques comporte deux disques (serveur 2 et serveur 3) dont la capacité est de 150 Go et de 120 Go, respectivement). La sauvegarde est exécutée une fois par jour sur le disque du serveur 2 et le snapshot est supprimé une fois les données copiées sur la bande. Sur le serveur 3, la sauvegarde est exécutée trois fois par jour et cinq snapshots différents sont utilisés tour à tour à des fins de restauration instantanée.

Figure 5-1 **Scénario de calcul de la capacité utilisée**



Le calcul de la capacité utilisée pour la sauvegarde avec temps d'indisponibilité nul tient compte de tous les disques utilisés lors des sessions de sauvegarde au cours des dernières vingt-quatre heures 200 Go (Serveur 1) + 150 Go (Serveur 2) + 120 Go (Serveur 3) = 470 Go.

La fonction de calcul de la capacité utilisée pour la restauration instantanée évalue la capacité source pour les sessions de sauvegarde avec temps d'indisponibilité nul ayant laissé des données à des fins de restauration instantanée. Le même disque n'est comptabilisé qu'une fois : 200 Go (Serveur 1) + 120 Go (Serveur 3) = 320 Go.

Licence de sauvegarde avancée sur disque

La licence de sauvegarde avancée sur disque est requise pour pouvoir réaliser une sauvegarde de la *bibliothèque de fichiers*. Il est possible de l'utiliser pour une bibliothèque de bandes virtuelle à la place des licences d'utilisation de lecteur et de bibliothèque.

Lors de la vérification d'une licence de sauvegarde avancée sur disque, la quantité d'espace utilisé sur l'ensemble des supports configurés sur les périphériques qui utilisent la licence de sauvegarde avancée sur disque est comparée au nombre de licences installées.

Vous devez disposer d'une licence de sauvegarde avancée sur disque pour chaque téra-octet de données sauvegardées sur tous les supports des bibliothèques de fichiers et des bibliothèques de bandes virtuelles. En ce qui concerne les bibliothèques de bandes virtuelles, on applique un taux de compression hypothétique de 2 pour 1. Cela signifie que vous pouvez sauvegarder jusqu'à 2 téra-octets de données avec une seule licence de sauvegarde avancée sur disque.

Des licences supplémentaires pour 10 To et 100 To sont également disponibles. Elles sont plus économiques que 10 licences de 1 To ou 100 licences de 1 To.

Si une bibliothèque de fichiers, une bibliothèque de bandes virtuelle ou un support virtuel est exporté à partir de la base de données IDB, les données de ce support ne sont plus décomptées dans la licence. L'importation d'un support (si les données n'ont pas été écrasées) entraîne le décompte des données de ce support pour la licence de sauvegarde avancée sur disque.

Au début de la sauvegarde ou de la copie d'objets, la quantité d'espace disque déjà occupée par les sessions de sauvegarde ou de copie d'objets précédentes est calculée. Si la valeur est inférieure ou égale à l'espace de sauvegarde sur disque autorisé par la licence, la sauvegarde démarre et se termine, indépendamment de la quantité de données en cours de sauvegarde (pouvant dépasser l'espace disque total). Si la limite a déjà été dépassée lors des sessions de sauvegarde précédentes, la session de sauvegarde démarre, mais un avertissement est émis pour indiquer que la limite de capacité autorisée par la licence a été dépassée.

Pour calculer l'espace disque occupé par la sauvegarde sur disque dans la cellule, Data Protector totalise les capacités de tous les supports créés lors des sauvegardes effectuées vers les bibliothèques de fichiers et les bibliothèques de bandes virtuelles au sein de la cellule.

La vérification d'une licence de sauvegarde avancée sur disque ne tient pas compte du nombre de périphériques, de lecteurs et d'emplacements, mais seulement de la quantité de données conservée dans la base de données IDB de Data Protector.

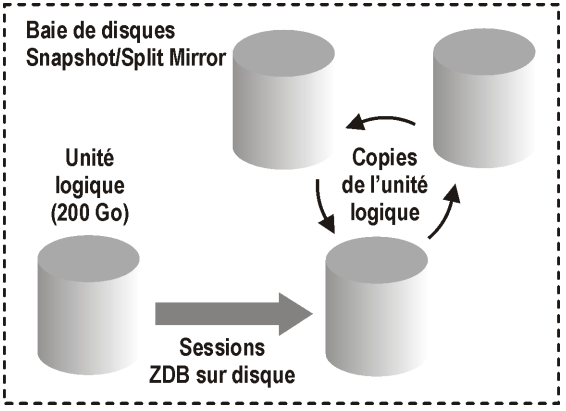
REMARQUE Par défaut, Data Protector traite les bibliothèques de bandes virtuelles comme des bibliothèques ordinaires (comme les bibliothèques SCSI II par exemple). Pour pouvoir utiliser les licences de sauvegarde avancée sur disque, il faut que le périphérique soit identifié comme bibliothèque de bandes virtuelle lors de sa configuration. Dans l'index de l'aide en ligne, recherchez : “bibliothèque de bandes virtuelle”.

Exemples d'attribution de licences basées sur la capacité

Ce paragraphe fournit des exemples illustrant la manière dont les licences basées sur la capacité sont attribuées.

Exemple 1 La figure 5-2 à la page 324 montre une situation dans laquelle les données d'une unité logique de 800 Go sont sauvegardées trois fois par jour au cours d'une session de sauvegarde avec temps d'indisponibilité nul sur disque.

Figure 5-2 Sessions de sauvegarde avec temps d'indisponibilité nul sur disque



Trois copies Split mirror ou snapshot (répliques) sont copiées en rotation et conservées à des fins de restauration instantanée. L'attribution de la licence basée sur la capacité est calculée de la manière suivante :

Une unité logique de 800 Go est utilisée pour les sessions de sauvegarde avec temps d'indisponibilité nul sur disque :

1 x 800 Go = 0,8 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

Trois copies de la même unité logique de 800 Go sont conservées à des fins de restauration instantanée. Notez que la licence tient compte de la capacité de stockage des volumes source et non de la capacité des répliques :

1 x 800 Go = 0,8 To pour la licence "Restauration instantanée pour 1 To".

Une licence “Sauvegarde à temps d'indisponibilité nul pour 1 To” et une licence “Restauration instantanée pour 1 To” suffisent pour le cas illustré par la figure 5-2 à la page 324.

Exemple 2

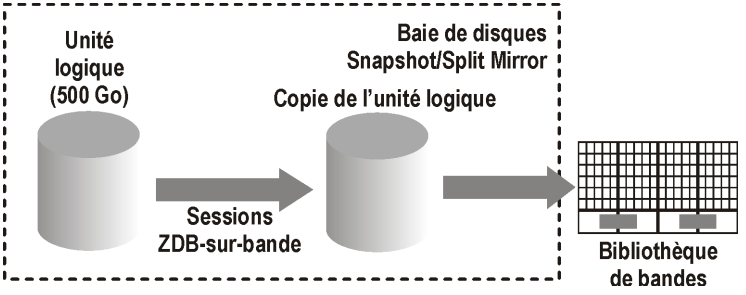
La figure 5-3 à la page 325 montre une situation dans laquelle les données d'une unité logique de 800 Go sont sauvegardées deux fois par jour au cours d'une session de sauvegarde avec temps d'indisponibilité nul sur bande. Par conséquent, les copies Split mirror ou snapshot (répliques) ne sont pas conservées à des fins de restauration instantanée. L'attribution de la licence basée sur la capacité est calculée de la manière suivante :

Une unité logique de 800 Go est utilisée pour les sessions de sauvegarde avec temps d'indisponibilité nul sur disque :

1 x 800 Go = 0,8 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

La licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To" suffit.

Figure 5-3 Sessions de sauvegarde avec temps d'indisponibilité nul sur bande



Exemple 3

La figure 5-4 à la page 326 montre une situation dans laquelle les données d'une unité logique de 800 Go sont sauvegardées trois fois par jour au cours d'une session de sauvegarde avec temps d'indisponibilité nul sur disque + bande. Cinq copies Split mirror ou snapshot (répliques) sont copiées en rotation et conservées à des fins de restauration instantanée. L'attribution de la licence basée sur la capacité est calculée de la manière suivante :

Une unité logique de 800 Go est utilisée pour les sessions avec temps d'indisponibilité nul sur disque + bande :

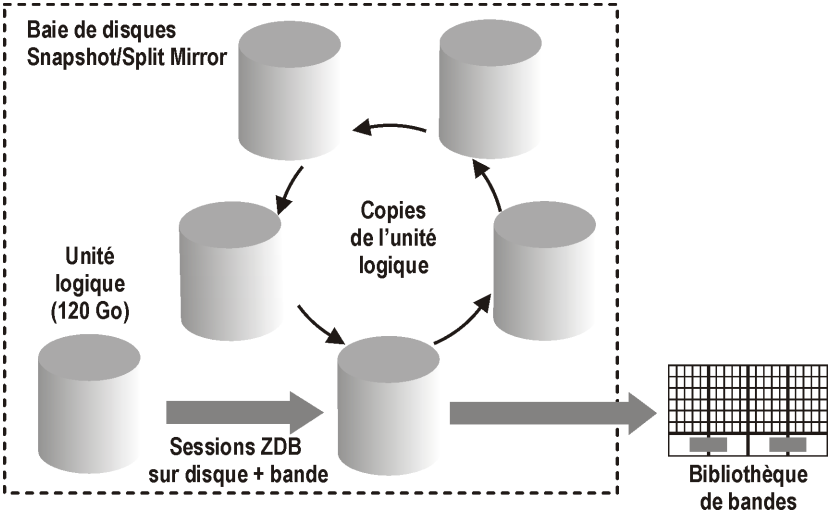
1 x 800 Go = 0,8 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

Cinq copies de la même unité logique de 800 Go sont conservées à des fins de restauration instantanée. Notez que la licence tient compte de la capacité de stockage des volumes source et non de la capacité des répliques :

1 x 800 Go = 0,8 To pour la licence "Restauration instantanée pour 1 To".

Une licence “Sauvegarde avec temps d'indisponibilité nul pour 1 To” et une licence “Restauration instantanée pour 1 To” suffisent.

Figure 5-4 **Sessions avec temps d'indisponibilité nul sur disque + bande**



Exemple 4

La figure 5-5 à la page 328 montre une situation dans laquelle les données d'une unité logique de 800 Go sont sauvegardées 4 fois par jour au cours d'une session de sauvegarde directe. Trois copies Split mirror ou snapshot (répliques) créées lors de la session de sauvegarde directe sont copiées en rotation et conservées à des fins de restauration instantanée. L'attribution de la licence basée sur la capacité est calculée de la manière suivante :

Une unité logique de 800 Go est utilisée pour les sessions de sauvegarde directe :

1 x 800 Go = 0,8 To pour la licence "Sauvegarde directe pour 1 To".

La même unité logique de 800 Go est utilisée pour les sessions de sauvegarde avec temps d'indisponibilité nul sur disque + bande. Elle est donc soumise à une autre licence :

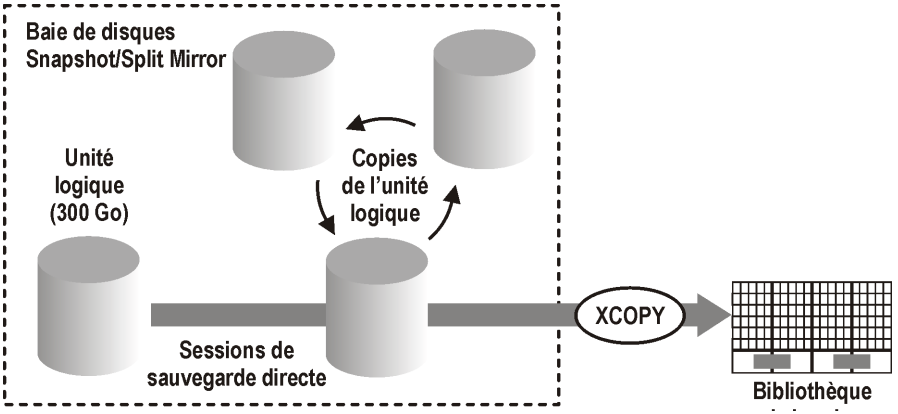
1 x 800 Go = 0,8 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

Trois copies de la même unité logique de 800 Go sont conservées à des fins de restauration instantanée. Notez que la licence tient compte de la capacité de stockage des volumes source et non de la capacité des répliques :

1 x 800 Go = 0,8 To pour la licence "Restauration instantanée pour 1 To".

Une licence “Sauvegarde directe pour 1 To”, une licence “Sauvegarde avec temps d'indisponibilité nul pour 1 To" et une licence "Restauration instantanée pour 1 To" suffisent pour le cas illustré par la figure 5-5 à la page 328.

Figure 5-5 **Sessions de sauvegarde directe**



Exemple 5

Une unité logique de 200 Go, une de 500 Go, une de 120 Go et une de 300 Go sont utilisées dans des sessions de sauvegarde avec temps d'indisponibilité nul :

1 x 200 Go + 1 x 500 Go + 1 x 120 Go + 1 x 300 Go = 1,12 To pour la licence “Sauvegarde avec temps d'indisponibilité nul pour 1 To”.

Des copies Split Mirror ou snapshot d'unités logiques de respectivement 200 Go, 120 Go et 300 Go sont conservées à des fins de restauration instantanée :

1 x 200 Go + 1 x 120 Go + 1 x 300 Go = 0,62 To pour la licence “Restauration instantanée pour 1 To”.

Une unité logique de 300 Go est utilisée dans les sessions de sauvegarde directe :

1 x 300 Go = 0,3 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

Une licence “Sauvegarde directe pour 1 To”, deux licences “Sauvegarde avec temps d'indisponibilité nul pour 1 To” et une licence “Restauration instantanée pour 1 To” suffisent si les quatre exemples dans les figures 5-2 à 5-6 sont configurés dans une cellule.

Production d'un rapport de licences sur demande

Pour générer un rapport sur les licences, utilisez la commande `omnicc` de Data Protector. Saisissez la commande suivante :

```
omnicc -check_licenses [-detail]
```

Si l'option `-detail` n'est pas spécifiée, les informations renvoyées par la commande indiquent si l'attribution de licences Data Protector est possible ou non.

Si l'option `-detail` est spécifiée, un rapport détaillé est généré. Les informations renvoyées pour chaque licence de la cellule sont les suivantes : nom de licence, licences installées, licences utilisées et licences requises.

Pour plus d'informations, reportez-vous à la page man `omnicc`. Notez que la commande n'indique pas les dates d'expiration des licences. Selon l'environnement et le nombre de licences installées, le rapport peut mettre un certain temps pour se générer. Pour obtenir les dates d'expiration des licences, saisissez la commande suivante :

```
omnicc -password_info
```

IMPORTANT

Dans un environnement MoM dans lequel la base de données CMMDB est configurée, il convient d'exécuter la commande `omnicc` sur le Gestionnaire de cellule sur lequel la base de données CMMDB est installée lors de la génération d'un rapport sur les licences pour les éléments liés aux bibliothèques et aux lecteurs.

Quelles sont les licences disponibles ?

Le tableau suivant présente les licences disponibles avec ce produit. Pour obtenir des informations détaillées sur chaque référence produit, reportez-vous à l'Annexe A du présent manuel.

Figure 5-6 Gamme des produits HP OpenView Storage Data Protector

1. packs starter	(obligatoire)	ttes plates-formes	Windows	Linux	HP-UX	Solaris
licence et DVD	1 x sys. gestion	B6960LA	B6961AA	B6961DA	B6951AA	B6951DA
manuels pack starter – version papier						
licence seule	1 x sys. gestion		B6961BA	B6961CA	B6951BA	B6951CA
jeu de DVD	comprend 2 DVD	B6960MA				
jeu de CD (DVD conseillés)	comprend 15 CD	B6960MB				

2. extensions lecteurs et bibliothèques		ttes plates-formes	Windows, NetWare, Linux	SAN, UNIX, NAS
licence lecteur	1 x lecteur		B6963AA	B6953AA
licence bibliothèque	1 x 61-250 empl./nb illim.	B6957BA/B6958BA		
	1 x mise à niv. emp. illim.	B6958CA		

3. extensions fonctionnelles		ttes plates-formes	Windows et Linux	UNIX
manuels pour ext. fonctionnelles – version papier		B6960EA		
licence de sauv. en ligne	1 x système		B6965BA	B6955BA
licence mgr-of-mgrs	1 x system		B6966AA	B6956AA
licence sauv. av. disque	1 x To/10 x To/100 x To	B7038AA/BA/CA		
lic. sauv. fich. ouverts	1 x serveur d'entreprise	BA155AA		
	1 x 1-serv./1 x 10-serv.	BA153AA/BA		
	5 x stations de travail	BA154AA		
	CD uniquement	BA152AA		
lic. opérations supports	1 x 2 000/10 000 supp.	B7100AA/B7101AA		
	1 x nbr illim. supp.	B7102AA		
	CD uniq./manuels uniq.	B7129AA/B7128AA		

		NDMP	HP XP	HP EVA	EMC
licence ZDB	1 x To /10 x To		B7023CA/DA	B7025CA/DA	B6959CA/DA
licence restaur. instant.	1 x To /10 x To		B7026CA/DA	B7028AA/DA	
licence sauv. directe	1 x To /10 x To	B7022BA/DA	B7027AA/DA		

édition serveur unique	Windows	HP-UX	Solaris
licence et supports / licence seule	B7030AA/BA	B7020AA/BA	B7020DA/CA
migration vers pack starter	B7031AA	B7021AA	B7021DA

NOUVEAU SKU avec Data Protector 6.0

Les nouveaux numéros de produits dans le tableau ci-dessus sont indiqués en rouge.

Data Protector utilise les numéros de produits des versions précédentes de Data Protector. C'est la raison pour laquelle les licences Data Protector existantes restent valides après la migration. Pour plus d'informations sur les licences disponibles, reportez-vous à la section “Structure de produit et licences Data Protector A.06.00” à la page A-2.

A propos des mots de passe

Vous trouverez ci-après des éléments qui vous aideront à déterminer le nombre de mots de passe dont vous avez besoin.

- Les mots de passe temporaires sont utilisables sur tout candidat à un Gestionnaire de cellule. En revanche, pour tous les autres types de mots de passe, vous devez déterminer la plate-forme correspondante. Cela s'applique également au Gestionnaire de cellule, qui deviendra le système d'administration central de Data Protector. Il est important d'utiliser des mots de passe temporaires pour appréhender parfaitement les besoins de votre configuration de cellule avant de demander un mot de passe permanent.
- Les licences permanentes peuvent être déplacées vers un autre Gestionnaire de cellule. En revanche, vous devez utiliser le ou les formulaires de déplacement de licence et les envoyer au *Centre de remise de mot de passe HP (PDC)*.
- Les mots de passe sont installés sur le Gestionnaire de cellule et sont valides pour l'intégralité de la cellule.
- La gestion centralisée des licences est assurée par la fonctionnalité Manager-of-Managers (MoM). Si vous achetez plusieurs licences pour différentes cellules, vous pouvez les installer sur le système MoM.
- Vous devez disposer d'une licence de Gestionnaire de cellule pour chaque cellule.
- Le logiciel vérifie que les licences sont toujours valables chaque fois que vous effectuez une tâche de configuration Data Protector ou que vous démarrez une session de sauvegarde.
- Les mots de passe temporaires sont utilisables sur tout système, tandis que les mots de passe d'évaluation et permanents ne sont utilisables que sur le système du Gestionnaire de cellule pour lequel vous avez demandé les licences.
- Si le système sur lequel le Gestionnaire de cellule est installé dispose de plusieurs adresses IP (systèmes multirésidents, serveurs RAS, clusters), vous pouvez lier la licence à n'importe laquelle de ces adresses IP.

REMARQUE

Si vous avez prévu de modifier l'adresse IP du Gestionnaire de cellule, de déplacer le Gestionnaire de cellule sur un autre système ou de déplacer les licences d'une cellule à une autre (et que vous n'utilisez pas la fonctionnalité MoM), vous devez contacter le *Centre de remise de mot de passe HP (PDC)* pour mettre vos licences à jour. Consultez la section “Autres moyens d'obtenir et d'installer des mots de passe permanents” à la page 336 pour connaître la procédure à suivre pour contacter le *Centre de remise de mot de passe* HP.

Mots de passe Data Protector

Une fois Data Protector installé sur votre réseau, vous pouvez l'utiliser pendant 60 jours. A l'issue de cette période, vous devez installer un mot de passe permanent sur le Gestionnaire de cellule afin d'activer le logiciel. Vous pouvez charger le logiciel sur le Gestionnaire de cellule Data Protector, mais vous ne pouvez pas effectuer de tâches de configuration sans mot de passe permanent, car les licences requises pour cette fonctionnalité Data Protector particulière requièrent ce type de mot de passe.

Les licences Data Protector requièrent l'un des mots de passe suivants :

✓ Mot de passe temporaire

Un mot de passe temporaire est généré pour le produit lors de sa première installation. Vous pouvez utiliser le logiciel pendant 60 jours à compter de son installation sur tout système pris en charge par Data Protector. Au cours de cette période, vous devez demander un mot de passe permanent au *Centre de remise de mot de passe HP* et l'installer.

✓ Mots de passe permanents

Data Protector est livré avec une licence *Attestation de droit* qui vous donne le droit d'obtenir un mot de passe permanent. Ce mot de passe vous permet de configurer une cellule Data Protector en fonction de votre stratégie de sauvegarde, à condition que vous ayez acheté les licences requises. Avant de demander un mot de passe permanent, vous devez déterminer quel système sera utilisé pour le Gestionnaire de cellule et définir la configuration nécessaire.

✓ Mot de passe d'urgence

Les mots de passe d'urgence sont disponibles si les mots de passe installés ne correspondent pas à la configuration système en raison d'une urgence. Ils permettront à tout système de fonctionner pendant une période de 120 jours.

Les mots de passe d'urgence sont délivrés par l'organisation de support. Ils doivent être demandés par les collaborateurs HP et ne sont remis qu'à ces derniers. Reportez-vous à votre centre de support ou au centre HP d'attribution des licences à l'adresse : http://webware.hp.com.

Les mots de passe d'urgence sont conçus pour permettre des opérations de sauvegarde tandis que la configuration système originale est reconstruite ou jusqu'à ce que l'installation soit déplacée vers un nouvel emplacement permanent. En cas de déplacement des licences, vous devez remplir un formulaire de déplacement de licence et l'adresser au *Centre de remise de mot de passe HP* ou consulter la page Web http://webware.hp.com sur laquelle les mots de passe peuvent être générés, déplacés, etc.

Il est recommandé de demander les mots de passe à l'aide de l'utilitaire *HP OpenView AutoPass*, qui peut être installé pendant le processus d'installation du Gestionnaire de cellule. Reportez-vous à la section “Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP OpenView AutoPass” à la page 334 pour connaître les instructions sur l'obtention de mots de passe avec l'utilitaire HP OpenView AutoPass une fois ce dernier installé pendant le processus d'installation du Gestionnaire de cellule.

Reportez-vous à la section “Autres moyens d'obtenir et d'installer des mots de passe permanents” à la page 336 pour des instructions sur l'obtention et l'installation d'un mot de passe par un autre moyen que l'utilitaire *HP OpenView AutoPass*.

Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP OpenView AutoPass

L'utilitaire HP OpenView AutoPass permet d'installer directement via Internet des mots de passe pour les licences achetées pour vos produits HP OpenView, à partir du serveur Web du Centre de remise de mot de passe HP. Consultez le manuel *HP OpenView AutoPass Licensing Guide* pour en savoir plus sur l'utilitaire HP OpenView AutoPass.

Configuration système requise

Pour obtenir et installer des mots de passe permanents à l'aide de l'utilitaire HP OpenView AutoPass, vous devez remplir les conditions suivantes :

- L'utilitaire HP OpenView AutoPass doit avoir été installé pendant l'installation du Gestionnaire de cellule à l'aide du script `omnisetup.sh` de Data Protector (systèmes UNIX) ou pendant l'installation du Gestionnaire de cellule (systèmes Windows).

- Sur MC/ServiceGuard, l'utilitaire HP OpenView AutoPass doit être installé sur tous les nœuds.
- Vous devez disposer d'une attestation de droit d'une licence permanente.
- Vous devez disposer du numéro de commande HP pour les licences achetées.
- Vous avez besoin de l'adresse IP du Gestionnaire de cellule du système Manager-of-Managers.

Limites

Les limites suivantes s'appliquent à l'utilitaire HP OpenView :

- L'utilitaire HP OpenView AutoPass n'est pas installé sur des systèmes d'exploitation Windows autres que x64 et Linux.
- Il *n'*est *pas* recommandé d'installer l'utilitaire HP OpenView AutoPass sur Microsoft Cluster, car il ne serait installé que sur un seul nœud et non sur tous.

Pour plus d'informations sur les conditions requises et limitations, reportez-vous au manuel *HP OpenView AutoPass Licensing Guide*.

Les mots de passe sont installés sur le Gestionnaire de cellule et sont valides pour l'intégralité de la cellule.

Procédure

Pour obtenir et installer un mot de passe permanent, procédez comme suit :

1. Rassemblez les informations nécessaires à l'obtention d'un mot de passe permanent. Consultez le manuel *HP OpenView Auto Pass Licensing Guide* pour connaître les informations requises.
2. Commandez le mot de passe en ligne à l'aide de l'utilitaire *HP OpenView AutoPass*. Pour lancer l'utilitaire *HP OpenView AutoPass*, exécutez la commande suivante sur le Gestionnaire de cellule :

REMARQUE

Dans un environnement Manager-of-Managers (MoM), la commande `omniinstlic` doit être exécutée soit sur le système MoM (si vous *utilisez* une attribution centralisée des licences Data Protector), soit sur le Gestionnaire de cellule auquel les mots de passe commandés et installés sont destinés (si vous *n'*utilisez *pas* l'attribution centralisée des licences Data Protector).

`/opt/omni/sbin/omniinstlic` (Gestionnaire de cellule UNIX) ou

<répertoire_Data_Protector>`\bin\omniinstlic` (Gestionnaire de cellule Windows)

Reportez-vous à la page man de `omniinstlic` pour plus d'informations.

3. Suivez les instructions de l'assistant *HP OpenView AutoPass* et saisissez les informations requises.

   A la dernière étape de l'assistant, cliquez sur `Obtenir mot de passe` pour transférer les mots de passe permanents des licences achetées du *Centre de remise de mot de passe HP* vers le Gestionnaire de cellule.

   Cliquez sur `Terminer` pour installer les mots de passe permanents des licences achetées sur le Gestionnaire de cellule.

4. Pour plus d'informations sur la vérification des mots de passe installés, reportez-vous à la section “Vérification du mot de passe” à la page 339.

Autres moyens d'obtenir et d'installer des mots de passe permanents

Obtention

Pour obtenir des mots de passe permanents, procédez comme suit :

1. Regroupez les informations demandées dans le *Formulaire de demande* de mot de passe permanent. Reportez-vous à la section “Formulaires d'attribution de licences Data Protector” à la page A-27 pour trouver l'emplacement des formulaires et obtenir des instructions pour les remplir.
2. Pour plus d'informations sur la structure des produits, reportez-vous à la section “Structure de produit et licences Data Protector A.06.00” à la page A-2. Le *Centre de remise de mot de passe HP* vous enverra un mot de passe permanent en utilisant la méthode dont vous vous êtes servi pour envoyer votre demande. Si vous avez fait votre demande par e-mail, par exemple, vous recevrez votre mot de passe permanent par e-mail.
3. Choisissez l'une des options suivantes :

   - Consultez le site Web du *Centre de remise de mot de passe HP* à l'adresse http://www.webware.hp.com.

- Remplissez le *Formulaire de demande de mot de passe permanent* et adressez-le au *Centre de remise de mot de passe HP* à l'aide d'une des méthodes suivantes (reportez-vous à l'attestation de droit livrée avec le produit pour connaître les numéros de téléphone et de télécopie, les adresses e-mail et les horaires d'ouverture) :

  — En envoyant le formulaire par télécopie au *Centre de remise de mot de passe HP*

  — En envoyant un e-mail au *Centre de remise de mot de passe HP*

  Vous pouvez également utiliser la version électronique des formulaires de licence qui se trouve dans les fichiers suivants sur le Gestionnaire de cellule et les supports de distribution :

  - Sous Windows : `<répertoire_Data_Protector>\Docs\license_forms.txt`
  - Sur le DVD-ROM *Windows* : `<Nom_disque>:\Docs\license_forms.txt`
  - Sous UNIX : `/opt/omni/doc/C/license_forms_UNIX`

  pour "copier" et "coller" votre message au *Centre de remise de mot de passe HP (HP PDC)*.

  Votre mot de passe permanent vous sera envoyé dans les 24 heures suivant l'envoi du *Formulaire de demande de mot de passe permanent.*

Installation

Les paragraphes qui suivent indiquent la procédure à suivre pour installer un mot de passe permanent transmis par le *Centre de remise de mot de passe HP (HP PDC)* :

Configuration système requise

Le *Centre de remise de mot de passe HP* doit vous avoir envoyé les mots de passe permanents et l'interface utilisateur Data Protector doit être installée sur le Gestionnaire de cellule. Les mots de passe sont installés sur le Gestionnaire de cellule et sont valides pour l'intégralité de la cellule.

Utilisation de l'interface graphique utilisateur

Pour installer le mot de passe permanent via l'interface graphique de Data Protector, procédez comme suit :

1. Dans le menu contextuel, cliquez sur `Clients`.

2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur `Cellule Data Protector`, puis sélectionnez `Ajouter licence`.
3. Vous devez saisir le mot de passe exactement tel qu'il figure dans le *Certificat de mot de passe*.

   Un mot de passe se compose de 8 groupes de 4 caractères chacun, séparés par un espace et suivis par une chaîne. Assurez-vous que cette séquence ne contient ni saut de ligne, ni retour chariot. Vous trouverez ci-après un exemple de mot de passe :

   ```
   4PXV EG9S B6WS 2VX3 5967 XEZK AAA9 MQJB "Product: B6965BA"
   ```

   Après avoir saisi le mot de passe, effectuez les vérifications suivantes :

   ✓ Assurez-vous que le mot de passe s'affiche correctement à l'écran.

   ✓ Vérifiez qu'il n'y a pas d'espace en tête ou à la fin du mot de passe, ni de caractères en trop.

   ✓ Vérifiez que vous n'avez pas confondu les caractères "1" (le chiffre) et "l" (la lettre).

   ✓ Vérifiez que vous n'avez pas confondu les caractères "O" (lettre majuscule) et "0" (chiffre).

   ✓ Vérifiez que vous avez respecté les majuscules et minuscules. Le mot de passe tient compte de la casse.

   Cliquez sur `OK`.

Le mot de passe est enregistré dans le fichier suivant :

- Sous Windows : *<répertoire_Data_Protector>*\Config\server\Cell\lic.dat
- Sous UNIX : /etc/opt/omni/server/cell/lic.dat

Utilisation de l'interface de ligne de commande

Pour installer le mot de passe permanent via l'interface de ligne de commande (CLI) de Data Protector, procédez comme suit :

1. Connectez-vous au Gestionnaire de cellule.
2. Exécutez la commande suivante :

   - Sous Windows :
     <répertoire_Data_Protector>\bin\omnicc -install_license *<mot de passe>*

- Sous UNIX :
  `/opt/omni/bin/omnicc -install_license <mot de passe>`

Le *<mot de passe>* doit être saisi tel qu'il apparaît dans le *Certificat de mot de passe*.

Vous pouvez également ajouter le mot de passe dans le fichier suivant :

- Sous Windows :
  <répertoire_Data_Protector>`\config\server\cell\lic.dat`
- Sous UNIX : `/etc/opt/omni/server/cell/lic.dat`

Si ce fichier n'existe pas, créez-en un avec un éditeur tel que `vi` ou `Bloc-notes`. Vous trouverez un exemple de mot de passe à l'étape 3 de la procédure faisant appel à l'interface graphique utilisateur.

Vérification du mot de passe

Utilisation de l'interface graphique utilisateur

Pour vérifier que le mot de passe pour la licence que vous avez installée est correct, procédez comme suit dans le Gestionnaire Data Protector :

1. Dans le menu `Aide`, cliquez sur `A propos de`.
2. Cliquez sur l'onglet `Licence`. Toutes les licences installées s'affichent. Si le mot de passe que vous avez saisi n'est pas correct, il est accompagné de la remarque `Impossible de décoder le mot de passe`.

Utilisation de l'interface de ligne de commande

Pour vérifier que le mot de passe pour la licence que vous avez installée est correct, utilisez la commande suivante :

- Sous Windows :
  <répertoire_Data_Protector>`\bin\omnicc -password_info`
- Sous UNIX : `/opt/omni/bin/omnicc -password_info`

Cette commande affiche toutes les licences installées. Si le mot de passe que vous avez saisi n'est pas correct, il est accompagné de la remarque `Impossible de décoder le mot de passe`.

Recherche du nombre de licences installées

Utilisation de l'interface graphique utilisateur

Après avoir installé un mot de passe permanent, vous pouvez vérifier le nombre de licences actuellement installées sur le Gestionnaire de cellule :

1. Démarrez le gestionnaire Data Protector.
2. Dans la barre de menus, cliquez sur `Aide`, puis sur `A propos`. La fenêtre `A propos du Gestionnaire` affiche alors les licences installées.

Utilisation de l'interface de ligne de commande

Si vous utilisez la ligne de commande, procédez comme suit :

1. Connectez-vous au Gestionnaire de cellule.
2. Exécutez la commande suivante :
   - Sous Windows : `<répertoire_Data_Protector>\bin\omnicc -query`
   - Sous UNIX : `/opt/omni/bin/omnicc -query`

Un tableau contenant les licences installées s'affiche alors.

Déplacement des licences vers un autre système Gestionnaire de cellule

Vous devez contacter le *Centre de remise de mot de passe HP* dans les cas suivants :

- Lorsque vous souhaitez déplacer le Gestionnaire de cellule vers un autre système.
- Lorsque vous prévoyez de déplacer vers une autre cellule Data Protector une licence installée sur un Gestionnaire de cellule qui n'est pas utilisé dans la cellule.

REMARQUE

Il est possible de déplacer une licence UNIX vers un autre Gestionnaire de cellule UNIX ou vers un Gestionnaire de cellule Windows ; en revanche, il est impossible de déplacer une licence Windows vers un Gestionnaire de cellule UNIX.

Procédez comme suit pour déplacer des licences d'un Gestionnaire de cellule vers un autre :

1. Remplissez un *Formulaire de déplacement de licence* pour chaque nouveau Gestionnaire de cellule et envoyez-le au *Centre de remise de mot de passe HP*. Si vous souhaitez déplacer des licences correspondant à des produits qui ne sont plus en vente, utilisez les *formulaires de déplacement de licence* fournis avec la version précédente du produit. Reportez-vous à la section “Formulaires d'attribution de licences Data Protector” à la page A-27.

   Dans le formulaire, vous devez spécifier le nombre de licences à déplacer du Gestionnaire de cellule existant.

2. Supprimez le fichier suivant :

   - Sous Windows : `<répertoire_Data_Protector>\config\server\cell\lic.dat`
   - Sous UNIX : `/etc/opt/omni/server/cell/lic.dat`

3. Après avoir rempli le *formulaire de déplacement de licence*, envoyez-le au *Centre de remise de mot de passe HP*. Vous êtes dans l'obligation légale de supprimer tous les mots de passe Data Protector du Gestionnaire de cellule courant.

4. Installez les nouveaux mots de passe. Vous recevrez un mot de passe pour chaque nouveau Gestionnaire de cellule. Vous recevrez également un nouveau mot de passe pour le Gestionnaire de cellule courant si des licences sont conservées sur celui-ci. Le nouveau mot de passe remplace le mot de passe utilisé sur le Gestionnaire de cellule courant.

Gestion centralisée des licences

Data Protector vous permet de configurer la gestion centralisée des licences pour l'environnement multicellules dans son intégralité, ce qui simplifie considérablement la gestion des licences. Toutes les licences sont conservées sur le système Manager-of-Managers (MoM) Manager. Elles sont ensuite allouées aux cellules spécifiques tout en restant configurées sur le Gestionnaire MoM.

Pour plus d'informations sur la procédure de configuration des licences, reportez-vous à l'aide en ligne de Data Protector.

REMARQUE Il est possible d'affecter une licence UNIX à un autre Gestionnaire de cellule UNIX ou à un Gestionnaire de cellule Windows ; en revanche, il est impossible d'affecter une licence Windows à un Gestionnaire de cellule UNIX.

La fonction MoM vous permet de déplacer (réaffecter) les licences entre les cellules MoM. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "environnement MoM".

Si vous installez une nouvelle licence Data Protector, n'oubliez pas de vérifier la fonctionnalité MoM avant de demander des licences. Si vous décidez d'utiliser la gestion centralisée de licences par la suite, vous devrez appliquer la procédure de déplacement des licences dans son intégralité.

REMARQUE La fonction MoM permet de gérer les licences de manière centralisée. Cela signifie que vous pouvez installer toutes les licences sur le Gestionnaire MoM, puis les distribuer aux Gestionnaires de cellule qui appartiennent à la cellule du MoM. Par la suite, les licences peuvent être déplacées (redistribuées) entre les cellules du MoM. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "environnement MoM".

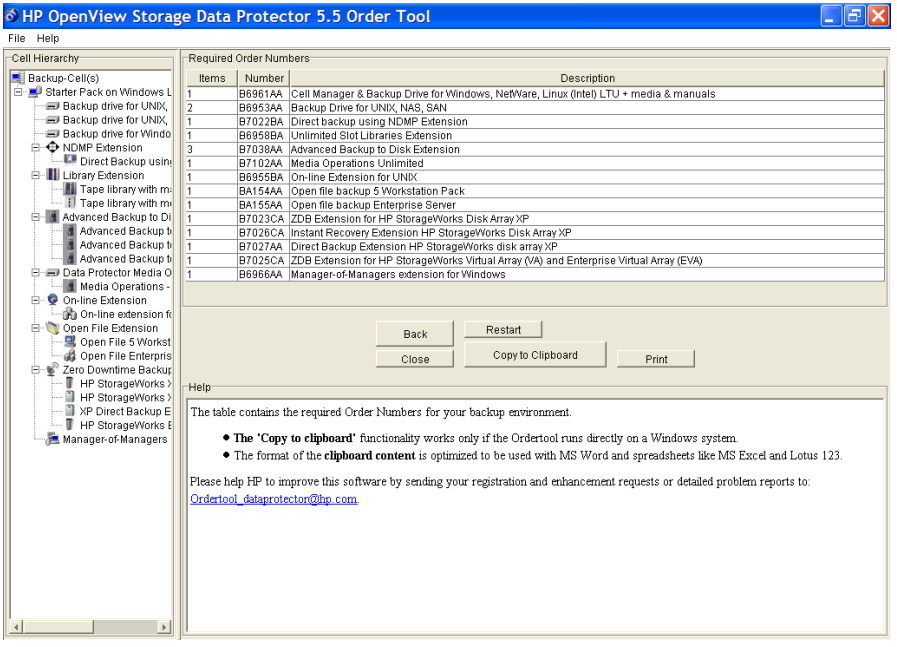
Outil de commande Data Protector

Data Protector comprend un outil simple permettant de générer automatiquement la liste des numéros de produits Data Protector requis pour votre environnement. Cet outil vous guide tout au long de la procédure : grâce à des questions simples concernant votre configuration système et l'utilisation envisagée, il est en mesure de déterminer la structure de votre cellule en fonction des réponses que vous lui avez données.

Une fois que vous avez répondu à toutes les questions, l'outil de commande affiche la liste complète des numéros de produits que vous devez commander pour l'environnement élaboré sur la base de vos réponses. Si vous souhaitez voir un exemple, reportez-vous à la figure 5-7 à la page 343.

L'outil de commande est disponible sur les DVD Data Protector.

Figure 5-7 Exemple de résultats fournis par l'outil de commande Data Protector



6 Résolution des problèmes d'installation

Description du chapitre

Ce chapitre contient des informations relatives aux problèmes d'installation. Vous trouverez des informations générales sur la résolution de problèmes dans le *Guide de dépannage HP OpenView Storage Data Protector*.

Ce chapitre contient des informations sur les éléments suivants :

Problèmes de résolution de noms lors de l'installation du Gestionnaire de cellule Windows

Au cours de l'installation du Gestionnaire de cellule Data Protector sous Windows, Data Protector détecte toute configuration erronée du DNS ou du fichier LMHOSTS et vous en avertit. De plus, Data Protector vous envoie une notification si le protocole TCP/IP n'est pas installé sur le système.

Problème

Echec de la résolution de noms avec le DNS ou le fichier LMHOSTS

Si la résolution de noms échoue, le message `"Erreur lors du développement du nom d'hôte"` s'affiche et l'installation est abandonnée.

- Si un problème de résolution survient lorsque vous utilisez le DNS, un message d'avertissement relatif à votre configuration DNS actuelle s'affiche.
- Si un problème de résolution survient lorsque vous utilisez le fichier LMHOSTS, un message d'avertissement s'affiche, vous invitant à vérifier le paramétrage de ce fichier.
- Si vous n'avez configuré ni l'un ni l'autre (DNS ou LMHOSTS), un message d'avertissement s'affiche pour activer le DNS ou la résolution LMHOSTS dans la boîte de dialogue des propriétés TCP/IP.

Action

Vérifiez la configuration du DNS ou du fichier LMHOSTS, ou activez-la. Reportez-vous à la section “Vérification des connexions DNS dans la cellule Data Protector” à la page 349.

Problème

Le protocole TCP/IP n'est pas installé et configuré sur votre système

Data Protector utilise le protocole TCP/IP pour les communications réseau ; celui-ci doit donc être installé et configuré sur chaque client de la cellule. Dans le cas contraire, l'installation est abandonnée.

Action

Vérifiez la configuration TCP/IP. Pour plus d'informations, reportez-vous à la section “Paramétrage du protocole TCP/IP sur les systèmes Windows” à la page B-21.

Vérification des connexions DNS dans la cellule Data Protector

Le DNS (Domain Name System) est un service de noms pour les hôtes TCP/IP. Le DNS est configuré avec une liste de noms d'hôtes et d'adresses IP, ce qui permet aux utilisateurs de désigner les systèmes distants par des noms d'hôtes plutôt que par des adresses IP. Le DNS garantit le bon fonctionnement des communications entre membres de la cellule Data Protector.

Si le DNS n'est pas correctement configuré, des problèmes de résolution de noms peuvent survenir dans la cellule Data Protector et les membres ne seront pas en mesure de communiquer les uns avec les autres.

Data Protector fournit la commande `omnicheck` pour vérifier les connexions DNS entre membres de la cellule Data Protector. Même si cette commande permet de vérifier toutes les connexions possibles dans la cellule, il suffit de vérifier les connexions suivantes, essentielles à la cellule Data Protector :

- Gestionnaire de cellule vers tout autre membre de la cellule et vice versa
- De l'Agent de support vers tout autre membre de la cellule et vice versa

Utilisation de la commande omnicheck

Limites

- La commande vérifie uniquement les connexions entre membres de la cellule, et non les connexions DNS en général.
- Elle ne peut être utilisée que sur les clients Data Protector sur lesquels Data Protector A.05.10 (ou une version ultérieure) est installé. Si la commande rencontre un client disposant d'une version antérieure de Data Protector, elle envoie un message d'erreur et reprend au client suivant.

La commande `omnicheck` réside dans le répertoire suivant du Gestionnaire de cellule :

Windows : `<répertoire_Data_Protector>\bin`

UNIX : `/opt/omni/bin`

Le synopsis de la commande `omnicheck` est le suivant :

```
omnicheck -dns [-host Client | -full] [-verbose]
```

Les différentes options vous permettent de vérifier les connexions DNS suivantes dans la cellule de Data Protector :

- Pour vous assurer que le Gestionnaire de cellule et que chaque Agent de support présent dans la cellule résolvent correctement les connexions DNS vers chaque client Data Protector de la cellule et vice versa, exécutez la commande suivante :

  ```
  omnicheck -dns [-verbose]
  ```

- Pour vérifier qu'un client Data Protector particulier résout correctement les connexions DNS avec chaque client Data Protector de la cellule, exécutez la commande suivante :

  ```
  omnicheck -dns -host <client> [-verbose]
  ```

  où *<client>* est le nom du client Data Protector vérifié.

- Pour vérifier toutes les connexions DNS possibles dans la cellule, exécutez la commande suivante :

  ```
  omnicheck -dns -full [-verbose]
  ```

Lorsque l'option `[-verbose]` est spécifiée, la commande retourne tous les messages. Si cette option n'est pas définie (réglage par défaut), seuls les messages résultant d'échecs de vérification sont retournés.

Pour plus d'informations, reportez-vous à la page `omnicheck` du manuel.

Le tableau 6-1 répertorie les messages retournés pour la commande `omnicheck`. Si le message retourné indique un problème de résolution DNS, reportez-vous au chapitre “Dépannage du réseau et de la communication” dans le *Guide de dépannage HP OpenView Storage Data Protector*.

Tableau 6-1 Messages retournés

Message retourné	Signification
client_1 ne peut pas se connecter à *client_2*	Délai de connexion à *client_2* dépassé.

Tableau 6-1 Messages retournés

Message retourné	Signification
client_1 se connecte à *client_2*, mais le système connecté se présente comme *client_3*	Le fichier *<%SystemRoot%>*\System32\drivers\etc\hosts (systèmes Windows) ou /etc/hosts (systèmes UNIX) n'est pas correctement configuré sur *client_1* ou le nom d'hôte de *client_2* ne correspond pas à son nom DNS.
client_1 n'a pas pu se connecter à *client_2*	*client_2* est inaccessible (c'est-à-dire déconnecté) ou le fichier *<%SystemRoot%>*\System32\drivers\etc\hosts (systèmes Windows) ou /etc/hosts (systèmes UNIX) n'est pas correctement configuré sur *client_1*.
vérification de la connexion entre *client_1* et *client_2*	
toutes les vérifications se sont terminées correctement.	
nb_vérifications_non_réussies échecs de vérification.	
le client n'est pas membre de la cellule.	
le client a été contacté, mais il s'agit apparemment d'une version antérieure. Le nom d'hôte n'est pas vérifié.	

Résolution des problèmes d'installation et de mise à niveau de Data Protector sous Windows

Problème

L'un des messages d'erreur suivants s'affiche

- `Le service Windows Installer est inaccessible.`
- `Cette application doit être installée pour que le programme s'exécute.`
- `Impossible d'ouvrir ce package de correctifs.`
- `Impossible d'ouvrir le périphérique ou le fichier spécifié.`

Après l'installation ou la mise à niveau vers Data Protector A.06.00, Windows peut signaler que certaines applications ne sont pas installées ou qu'il est nécessaire de les réinstaller.

Ce problème est dû à une erreur de la procédure de mise à niveau de Microsoft Installer. Les données de la version 1.x de Microsoft Installer n'ont pas été transférées vers la version 2.x de Microsoft Installer que Data Protector installe sur l'ordinateur.

Action

Ce problème est décrit à l'article Q324906 de la base de connaissances Microsoft.

Problème

Echec de l'installation d'un Gestionnaire de cellule sur un système Windows qui ne fait partie d'aucun domaine Windows

Le message d'erreur suivant s'affiche :

`Impossible de faire correspondre le mot de passe et le nom de compte spécifié.`

Actions

Deux solutions possibles :

- Associer le système Windows sur lequel vous installez le Gestionnaire de cellule à un domaine.
- Utiliser le compte administrateur local pour le service CRS.

Problème **Le message d'erreur suivant s'affiche :**

```
Fichier msvcr71.dll introuvable
```

Impossible de trouver la bibliothèque `MSVCR71.dll` (en majuscules), car il n'y a que `msvcr71.dll` (en minuscules) sur le partage réseau. Comme `MSVCR71.dll` et `msvcr71.dll` sont traités comme des fichiers différents, `setup.exe` n'arrive pas à trouver la bonne `dll`.

Action Renommez le fichier `msvcr71.dll` (minuscules) en `MSCVCR71.dll` (majuscules) ou reconfigurez le partage réseau de façon à ce qu'il ne soit plus sensible à la casse.

Problèmes lors de l'installation à distance des clients Windows

Problème **Erreur lors du lancement du processus d'installation**

Lorsque vous utilisez l'installation à distance Data Protector pour mettre à jour les clients Windows, le message d'erreur suivant s'affiche :

```
Erreur au démarrage du processus d'installation, err=[1326]
Accès réseau refusé : nom d'utilisateur inconnu ou mauvais
mot de passe.
```

Le problème est que le service `Inet Data Protector` fonctionne sur l'ordinateur distant sous un compte utilisateur qui ne dispose pas d'un accès au partage OmniBack II sur l'ordinateur du Serveur d'installation. Il s'agit très probablement d'un utilisateur local.

Action Remplacez l'utilisateur pour le service `Inet Data Protector` par un utilisateur qui puisse accéder au partage Data Protector.

Résolution des problèmes d'installation du Gestionnaire de cellule Data Protector sous Solaris

Problème

Impossible de créer un répertoire temporaire

Lors de l'installation de Gestionnaire de cellule sous Solaris, un répertoire temporaire ne peut être créé et l'installation échoue avec le message d'erreur suivant :

```
Processing package instance <OB2-CORE> from
</tmp/DP_A0510_158_SUN78.pkg>

pkgadd: ERREUR : unable to make temporary directory
<//tmp/old//installR.aOj3>
```

Action

Créez manuellement le répertoire temporaire manquant à l'emplacement indiqué dans le message d'erreur et redémarrez la procédure d'installation.

Par exemple, si vous obtenez le message d'erreur ci-dessus, créez le répertoire suivant : `//tmp/old//installR.aOj3`.

Résolution des problèmes d'installation des clients UNIX

Problème

Echec de l'installation à distance de clients UNIX

L'installation ou la mise à niveau à distance d'un client UNIX échoue avec le message d'erreur suivant :

```
Installation/Upgrade session finished with errors.
```

Lors de l'installation ou de la mise à niveau à distance de clients UNIX, l'espace disque disponible sur un système client dans le dossier `/tmp` doit atteindre au moins la taille du plus gros package à installer. Sur les systèmes client Solaris, la même quantité d'espace disque doit également être disponible dans le répertoire `/var/tmp`.

Action

Vérifiez si vous disposez de suffisamment d'espace disque dans ces répertoires et redémarrez la procédure d'installation ou de mise à niveau.

Pour connaître l'espace disque nécessaire, reportez-vous au document *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*.

Problème

Problèmes d'installation d'un client HP-UX

Lorsque vous ajoutez un nouveau client HP-UX à une cellule Data Protector, le message d'erreur suivant s'affiche :

```
/tmp/omni_tmp/packet: vous ne disposez pas des autorisations
requises pour exécuter cette fonction SD...
```

```
Accès refusé à root pour démarrer l'agent sur le dépôt
enregistré /tmp/omni_tmp/packet. Insertion non autorisée sur
l'hôte.
```

Action

Arrêtez le démon `swagent` et relancez-le, soit en supprimant le processus, soit en le redémarrant à l'aide de la commande `/opt/omni/sbin/swagentd` ou `/opt/omni/sbin/swagentd -r`.

Vérifiez que vous disposez d'une entrée de bouclage local (localhost) dans le fichier hosts (`/etc/hosts`).

Problème

Impossible de démarrer Omniinet après l'installation du Gestionnaire de cellule Unix

Au démarrage du Gestionnaire de cellule, le message d'erreur suivant s'affiche :

```
ERREUR :   Impossible de démarrer le service "omniinet",
erreur système : [1053] erreur inconnue 1053.
```

Action

Vérifiez que le service `inetd` ou `xinetd` est en cours d'exécution :

HP-UX et Solaris : `ps -ef | grep inetd`

Linux : `ps -ef | grep xinetd`

Pour démarrer le service, exécutez :

HP-UX : `/usr/sbin/inetd`

Solaris : `/usr/sbin/inetd -s`

Linux : `rcxinetd start`

Vérification de l'installation du client Data Protector

La vérification de l'installation du client Data Protector se divise en plusieurs étapes :

- Vérification de la configuration DNS des systèmes Gestionnaires de cellule et clients, puis vérification que les résultats de la commande `omnicheck -dns` du système Gestionnaire de cellule et client correspondent au système spécifié.
- Vérification des composants logiciels installés sur le client.
- Comparaison de la liste des fichiers requis pour un composant logiciel particulier à installer avec celle des fichiers présents sur le client.
- Vérification du total de contrôle pour chaque fichier en lecture seule requis pour un composant logiciel particulier.

Condition préalable

Un Serveur d'installation doit être disponible pour le type de système client (UNIX, Windows) sélectionné.

Limites

La procédure de vérification ne s'applique pas aux clients Novell NetWare et MPE.

Pour vérifier une installation Data Protector à l'aide de l'interface graphique de Data Protector, procédez comme suit :

1. Dans le menu contextuel, cliquez sur `Clients`.
2. Dans la fenêtre de navigation, développez `Clients`, cliquez sur le système du Gestionnaire de cellule avec le bouton droit de la souris, puis cliquez sur `Vérifier installation` pour lancer l'assistant.
3. Suivez les instructions de l'assistant pour vérifier l'installation des systèmes dans la cellule. La fenêtre `Vérifier installation` s'affiche avec les résultats de l'installation.

   Reportez-vous à l'aide en ligne pour plus d'informations.

Si votre installation a échoué, reportez-vous à la section “Utilisation des fichiers journaux” à la page 361.

Pour plus d'informations sur la vérification de l'installation sur les systèmes UNIX à l'aide de l'interface en ligne de commande de Data Protector, reportez-vous à la page `ob2install` du manuel.

Dépannage de la mise à niveau

Problème

Les fichiers de la base de données IDB et de configuration ne sont plus disponibles après la mise à niveau

Après la mise à niveau du Gestionnaire de cellule à partir d'une version précédente, la base IDB ainsi que tous les fichiers de configuration ne sont pas disponibles. Ce problème survient en cas d'interruption de la procédure de mise à niveau, quelle qu'en soit la raison.

Action

Restaurez OmniBack II/Data Protector à partir de la sauvegarde effectuée avant la mise à niveau, éliminez la raison de l'interruption et redémarrez la mise à niveau.

Problème

Les anciens correctifs Data Protector ne sont pas supprimés après la mise à niveau

Les anciens correctifs Data Protector sont répertoriés dans la liste des programmes installés si vous exécutez la commande `swlist` une fois la mise à niveau Data Protector terminée. Les correctifs ont été supprimés du système au cours de la mise à niveau, mais restent dans la base de données sw.

Pour savoir quels correctifs Data Protector sont installés, reportez-vous à la section “Contrôle des correctifs Data Protector installés” à la page 225.

Action

Pour supprimer les anciens correctifs de la base de données sw, exécutez la commande suivante :

```
swmodify -u <correctif>.\* <correctif>
```

Par exemple, pour supprimer le correctif “`PHSS_30143`” de la base de données sw, exécutez la commande suivante :

```
swmodify -u PHSS_30143.\* PHSS_30143
```

Procédure de mise à niveau manuelle

Normalement, vous mettez à niveau les Gestionnaire de cellule et Serveur d'installation Data Protector A.05.00, Data Protector A.05.10 ou Data Protector A.05.50 UNIX en exécutant la commande `omnisetup.sh`, qui effectue une procédure automatique de mise à niveau. Il est toutefois possible d'effectuer une mise à niveau manuelle. Reportez-vous à la section “Mise à niveau sur des systèmes HP-UX et Solaris à l'aide d'outils natifs” à la page 18.

Utilisation des fichiers journaux

Si l'installation de Data Protector pose un problème, vous pouvez consulter l'un des fichiers journaux suivants pour le diagnostiquer :

- Journaux d'installation (Windows)
- Journaux système (UNIX)
- Fichiers journaux Data Protector

En cas de problème lors de l'installation, vous devrez consulter les fichiers journaux correspondant à votre type d'installation (en local ou à distance) et au système d'exploitation que vous utilisez.

Installation en local

Si vous rencontrez des difficultés lors d'une installation en local, reportez-vous aux fichiers journaux suivants :

Sur le Gestionnaire de cellule HP-UX :

- `/var/adm/sw/swinstall.log`
- `/var/adm/sw/swagent.log` (pour plus d'informations)

Sur le Gestionnaire de cellule Solaris et Linux :

`/var/opt/omni/log/debug.log`

Sur les clients Windows (sur le système sur lequel tourne le programme d'installation) :

- *<Temp>*`\OB2SetupLauncher.log`
- *<Disque_système>*`:\`*<Temp>*`\OB2_Setup_ui_`*<Date>*`_`*<Heure>*`.txt`
- *<Temp>*`\OB2DBG_`*<did>*`__setup_`*<Hôte>*`<`*num_débogage*`>.txt` (pour plus d'informations)

  où :

  — *<did>* (ID de débogage) est l'ID de processus du premier processus acceptant les paramètres de débogage. Cet ID est également l'ID de la session de débogage. Tous les autres processus utiliseront cet ID.

— *<Host>* est le nom de l'hôte sur lequel le fichier de trace est créé.

— *<num_débogage>* est un numéro généré par Data Protector.

L'emplacement du répertoire *<Temp>* est spécifié par la variable d'environnement TEMP. Pour connaître la valeur de cette variable, exécutez la commande `set`.

Installation à distance

Si vous rencontrez des difficultés lors d'une installation à distance, reportez-vous aux fichiers journaux suivants :

Sur le Serveur d'installation UNIX :

`/var/opt/omni/log/IS_install.log`

Sur les clients Windows (uniquement sur le système client à distance) :

- *<Temp>*`\INSTALL_SERVICE*.*`
- *<Disque_système>*`:\`*<Temp>*`\OB2_Setup_exe_`*<Date>*`_`*<Heure>*`.txt`

où *<Temp>* est un répertoire spécifié dans la variable d'environnement TEMP.

Si les fichiers journaux n'ont pas été créés, exécutez l'installation à distance avec l'option de débogage. Reportez-vous à la section “Création de traces d'exécution de l'installation” à la page 364.

Fichiers journaux Data Protector

Les fichiers journaux Data Protector répertoriés ci-dessous se trouvent dans :

Windows : *<répertoire_Data_Protector>*`\log`

HP-UX, Solaris et Linux : `/var/opt/omni/log` et `/var/opt/omni/server/log`

Autre système UNIX : `/usr/omni/log`

Novell NetWare : `SYS:\USR\OMNI\LOG`

Les fichiers journaux suivants sont importants pour la résolution des problèmes d'installation :

`debug.log` Contient des conditions inattendues. Bien que

certaines pourront vous servir, ces informations sont surtout destinées au service de support.

`inet.log` Contient des demandes effectuées auprès du service `inet` Data Protector. Il peut être utile pour contrôler les dernières activités de Data Protector sur les clients.

`IS_install.log` Contient une trace d'installation à distance et se trouve sur le Serveur d'installation.

`omnisv.log` Contient des informations relatives au démarrage et à l'arrêt des services Data Protector.

`upgrade.log` Ce journal est créé lors de la mise à niveau et contient des messages relatifs à la mise à niveau de la partie centrale (UCP) et à la mise à niveau de la partie concernant les détails (UDP).

`OB2_Upgrade.log` (UNIX uniquement) Ce fichier, créé lors de la mise à niveau, contient les traces de la procédure de celle-ci.

Pour obtenir des informations sur d'autres fichiers journaux, reportez-vous au *Guide de dépannage HP OpenView Storage Data Protector*.

Création de traces d'exécution de l'installation

Exécutez l'installation avec l'option de débogage si le service support clientèle HP vous le demande. Pour plus d'informations sur le débogage, notamment sur les options de débogage ci-dessous, et sur la préparation des données à envoyer au service support clientèle HP, reportez-vous au *Guide de dépannage HP OpenView Storage Data Protector*.

Windows :

Pour déboguer une installation à distance sur un système Windows, exécutez l'interface graphique utilisateur de Data Protector en utilisant l'option de débogage :

```
Manager -debug 1-99 <Suffixe_débogage>
```

Une fois la session terminée/abandonnée, récupérez les résultats du débogage dans les fichiers suivants :

- Sur le système du Serveur d'installation :

  <répertoire_Data_Protector>\tmp\OB2DBG_*<did>*__BM_*<Serveur_installation><num_débogage><Suffixe_débogage>*

- Sur le système distant :

  <Disque_système>:*<Temp>*\OB2DBG_*<did>*__INSTALL_SERVICE *<Nom_de_l'hôte><num_débogage><Suffixe_débogage>*

UNIX :

Pour procéder au débogage de l'installation sur un système UNIX, exécutez l'interface graphique utilisateur de Data Protector en utilisant l'option de débogage :

```
xomni -debug 1-99 <Suffixe_débogage>
```

ou

```
xomniadmin -debug 1-99 <Suffixe_débogage>
```

Une fois la session terminée/abandonnée, récupérez les résultats du débogage dans le répertoire tmp du système du Serveur d'installation.

A Annexe A

Structure de produit et licences Data Protector A.06.00

Cette annexe décrit la structure du produit Data Protector en détails afin de faciliter la commande et le repérage des numéros de produit.

La structure du produit se divise en différentes sections, comme l'indique la figure A-1 à la page A-3. Lorsque vous commandez une solution Data Protector, suivez la procédure suivante :

1. Sélectionnez un Pack Starter. Le numéro de produit approprié dépend du système d'exploitation de votre Gestionnaire de cellule.
2. Déterminez le nombre de lecteurs configurés dans votre environnement et les bibliothèques de bandes associées.
3. Identifiez les autres fonctions dont vous avez besoin. Les licences recommandées peuvent concerner aussi bien la fonction de sauvegarde en ligne que la fonction de restauration instantanée.

Vous devez au moins vous procurer une licence et des supports Pack Starter.

REMARQUE Les licences fournies pour les produits UNIX peuvent s'appliquer à tous les systèmes d'exploitation.

Figure A-1 Structure de produits HP OpenView Storage Data Protector

1. packs starter	(obligatoire)	ttes plates-formes	Windows	Linux	HP-UX	Solaris
licence et DVD	1 x sys. gestion	B6960LA	B6961AA	B6961DA	B6951AA	B6951DA
manuels pack starter – version papier						
licence seule	1 x sys. gestion		B6961BA	B6961CA	B6951BA	B6951CA
jeu de DVD	comprend 2 DVD	B6960MA				
jeu de CD (DVD conseillés)	comprend 15 CD	B6960MB				

2. extensions lecteurs et bibliothèques		ttes plates-formes	Windows, NetWare, Linux	SAN, UNIX, NAS
licence lecteur	1 x lecteur		B6963AA	B6953AA
licence bibliothèque	1 x 61-250 empl./nb illim.	B6957BA/B6958BA		
	1 x mise à niv. emp. illim.	B6958CA		

3. extensions fonctionnelles		ttes plates-formes	Windows et Linux	UNIX
manuels pour ext. fonctionnelles – version papier		B6960EA		
licence de sauv. en ligne	1 x système		B6965BA	B6955BA
licence mgr-of-mgrs	1 x system		B6966AA	B6956AA
licence sauv. av. disque	1 x To/10 x To/100 x To	B7038AA/BA/CA		
lic. sauv. fich. ouverts	1 x serveur d'entreprise	BA155AA		
	1 x 1-serv./1 x 10-serv.	BA153AA/BA		
	5 x stations de travail	BA154AA		
	CD uniquement	BA152AA		
lic. opérations supports	1 x 2 000/10 000 supp.	B7100AA/B7101AA		
	1 x nbr illim. supp.	B7102AA		
	CD uniq./manuels uniq.	B7129AA/B7128AA		

		NDMP	HP XP	HP EVA	EMC
licence ZDB	1 x To /10 x To		B7023CA/DA	B7025CA/DA	B6959CA/DA
licence restaur. instant.	1 x To /10 x To		B7026CA/DA	B7028AA/DA	
licence sauv. directe	1 x To /10 x To	B7022BA/DA	B7027AA/DA		

édition serveur unique	Windows	HP-UX	Solaris
licence et supports / licence seule	B7030AA/BA	B7020AA/BA	B7020DA/CA
migration vers pack starter	B7031AA	B7021AA	B7021DA

NOUVEAU SKU avec Data Protector 6.0

Les nouveaux numéros de produits dans le tableau ci-dessus sont indiqués en rouge.

Packs Starter

Le tableau A-1 contient les numéros de licence des Packs Starter Data Protector A.06.00.

Tableau A-1 Numéros de licence des Packs Starter HP OpenView Storage Data Protector

B6951AA	DVD et licence d'utilisation pour HP-UX
B6951BA	Licence d'utilisation uniquement pour HP-UX
B6951DA	DVD et licence d'utilisation pour Sun Solaris
B6951CA	Licence d'utilisation uniquement pour Sun Solaris
B6961AA	DVD et licence d'utilisation pour Windows
B6961BA	Licence d'utilisation uniquement pour Windows
B6961DA	DVD et licence d'utilisation pour Linux
B6961CA	Licence d'utilisation uniquement pour Linux
B6960MA	Kit DVD
B6960LA	Manuels Pack Starter - imprimés (anglais)
B6960LJ	Manuels Pack Starter - imprimés (japonais)
B6960LF	Manuels Pack Starter - imprimés (français)

La licence d'utilisation du Pack Starter inclut une licence pour :

- un Gestionnaire de cellule sur la plate-forme indiquée ;
- un nombre illimité d'Agents de sauvegarde sur n'importe quelle plate-forme ;
- une licence Lecteur (B6951xx contient 1xB6953AA et B6961xx contient 1xB6963AA) ;
- la gestion de supports intégrée ;
- les bibliothèques comportant 60 emplacements au maximum ;

- les options de récupération après sinistre ;
- la génération avancée de rapports (dans l'interface graphique utilisateur de Data Protector et via le Web) ;
- le support SAN (avec le Gestionnaire de cellule sous HP-UX ou Solaris) ;
- la gestion centrée service via les intégrations à HP OpenView.

Supports

Data Protector A.06.00 est livré sur deux DVD. Si vous avez besoin de CD, il existe aussi un kit CD (B6960MB) qui contient 15 CD. Il est toutefois recommandé d'utiliser le kit DVD.

Manuels

Tous les manuels sont disponibles sur les DVD, les CD et sur le site http://www.hp.com/support/manuals.

Vous pouvez commander des manuels imprimés avec les deux options suivantes : Pack Starter et Extensions fonctionnelles. Les manuels Pack Starter imprimés comportent :

- *Guide conceptuel HP OpenView Storage Data Protector*
- *Guide d'installation et de choix des licences HP OpenView Storage Data Protector*
- *Guide de dépannage HP OpenView Storage Data Protector*
- *Guide de récupération après sinistre HP OpenView Storage Data Protector*
- *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*

REMARQUE

Après avoir passé commande en utilisant les numéros de produits correspondant au DVD et à la licence d'utilisation, vous recevez un coffret DVD qui contient les DVD, la licence d'utilisation et le *Guide de démarrage rapide HP Data Protector*. Cette livraison ne comprend pas d'autres manuels imprimés. Par contre, les manuels sont disponibles

sous forme électronique sur le DVD ou sur le site http://www.hp.com/support/manuals et peuvent également être commandés séparément.

Extensions de lecteur et de bibliothèque

Les licences suivantes concernent un seul lecteur. Vous avez besoin d'autant de licences que de lecteurs utilisés à tout moment. Il s'agit généralement du nombre total de lecteurs configurés, ce qui permet une utilisation simultanée de tous les lecteurs.

Un lecteur de sauvegarde peut être un lecteur de bande, une unité logique sur disque (sauvegarde sur disque à l'aide d'un périphérique de fichier), ou un lecteur magnéto-optique. Il est possible d'accéder au lecteur et de le gérer en local ou via le réseau à partir d'un système disposant de n'importe quelle licence Data Protector.

Les licences de lecteurs ne peuvent pas être partagées par plusieurs cellules.

Pour connaître les lecteurs pris en charge, reportez-vous aux matrices de support Data Protector sous Specifications à l'adresse http://www.hp.com/go/dataprotector.

Le tableau A-2 contient le numéro de licence des extensions de lecteur Data Protector A.06.00 et le tableau A-4 celui des extensions de bibliothèque Data Protector A.06.00.

Tableau A-2 Extensions de lecteur HP OpenView Storage Data Protector

B6953AA	pour SAN, UNIX et NAS

Comprend la licence d'utilisation (LTU) pour un lecteur de sauvegarde connecté directement à un système UNIX, un périphérique NAS, utilisé dans un environnement SAN ou pour la sauvegarde sans serveur.

Les lecteurs connectés aux systèmes MPE de HP et OpenVMS requièrent cette licence.

Cette licence d'utilisation est également requise pour les configurations suivantes :

Systèmes NAS gérés via NDMP (par exemple, les serveurs de fichiers Network Appliance et EMC Celerra) ou systèmes NAS nécessitant un serveur de périphérique Data Protector propriétaire (Agent de support), HP Storage Works NAS 8000, par exemple.

Les systèmes NAS sous Windows, NetWare ou Linux standard pouvant exécuter un serveur de périphérique Data Protector standard (Agent de support) requièrent uniquement des extensions de lecteur Data Protector pour Windows, NetWare et Linux (B6963AA).

Elle peut aussi être utilisée pour les lecteurs uniques connectés à des systèmes Windows, NetWare et Linux. Toutefois, dans les cas où le lecteur n'est pas utilisé dans un SAN, la licence B6963AA constitue une solution plus économique.

Tableau A-3 Extensions de lecteur HP OpenView Storage Data Protector

B6963AA	pour Windows, NetWare et Linux

Comprend la licence d'utilisation (LTU) pour un lecteur de sauvegarde supplémentaire connecté directement à un système Windows, NetWare ou Linux (Intel).

Cette licence est valable pour les lecteurs connectés à des périphériques NAS sous Windows, NetWare ou Linux qui peuvent exécuter un Agent de support Data Protector standard.

Vous avez besoin d'autant de licences que de disques utilisés à tout moment. Il s'agit généralement du nombre total de lecteurs configurés permettant une utilisation simultanée de tous les lecteurs.

Pour connaître les lecteurs pris en charge, reportez-vous aux matrices de support Data Protector sous Specifications à l'adresse www.hp.com/go/dataprotector.

Tableau A-4 Extensions de bibliothèque HP OpenView Storage Data Protector

B6957BA	pour les bibliothèques de 61 à 250 emplacements
B6958BA	pour les bibliothèques avec un nombre illimité d'emplacements
B6958CA	licence de mise à niveau avec nombre illimité d'emplacements

La licence d'utilisation des extensions de bibliothèque inclut la licence pour la gestion des bibliothèques de bandes dans une cellule Data Protector. Vous devez disposer d'une licence par bibliothèque.

- Les silos StorageTek utilisant les systèmes de bibliothèque ACSLS et GRAU/EMASS et utilisant le DAS requièrent la licence B6958BA.
- Dans le cas où plusieurs cellules se partagent une bibliothèque, la licence d'utilisation Manager-of-Managers est requise pour chaque cellule afin qu'une seule licence couvre la bibliothèque sur toutes les cellules.
- Cette licence prend en compte les emplacements physiques à l'intérieur de la bibliothèque et non les emplacements logiques.
- Les bibliothèques permettant de créer des partitions virtuelles nécessitent également une licence basée sur le nombre d'emplacements physiques disponibles par bibliothèque physique.

  Exemples :

  — Une bibliothèque de 120 emplacements utilisée dans une seule cellule divisée en deux bibliothèques de 60 emplacements nécessite une licence B6957BA.

  — Une bibliothèque de 300 emplacements partagée par trois cellules (sans Manager-of-Managers) utilisant chacune 100 emplacements nécessite une licence B6957BA pour chaque cellule.

  — Une bibliothèque de 300 emplacements partagée par cinq cellules (sans Manager-of-Managers) utilisant chacune 60 emplacements ne nécessite aucune licence de bibliothèque.

  — Une bibliothèque de 300 emplacements partagée par trois cellules utilisant chacune 100 emplacements et gérées de façon centralisée via Manager-of-Managers avec gestion centrale des supports et des licences, nécessite une licence B6958BA pour toutes les cellules.

Pour connaître les bibliothèques prises en charge, reportez-vous aux matrices de support Data Protector sous Specifications à l'adresse www.hp.com/go/dataprotector.

Extensions fonctionnelles

Les tableaux de cette section contiennent les numéros de licence des extensions fonctionnelles Data Protector A.06.00.

Tableau A-5 Extension en ligne HP OpenView Storage Data Protector

B6955BA	pour UNIX
B6965BA	pour Windows ou Linux

La licence d'utilisation de l'extension de sauvegarde en ligne inclut la licence nécessaire pour effectuer la sauvegarde en ligne des bases de données et des applications qui s'exécutent sur la plate-forme spécifiée.

- Si un système exécute plusieurs partitions, cette licence d'utilisation est requise pour chaque partition.
- Dans un environnement de clusters, chaque système participant au cluster doit disposer de cette licence d'utilisation.
- Les licences de sauvegarde en ligne sont requises pour les sauvegardes avec temps d'indisponibilité nul (ZDB).
- La fonctionnalité d'image instantanée VSS (Volume Shadow copy Service) du système de fichiers Windows 2003 est prise en charge sans supplément de prix. Cependant, la sauvegarde en ligne des bases de données qui ne font pas partie du système d'exploitation requièrent cette extension de sauvegarde en ligne. La sauvegarde de la configuration système ne requiert pas d'extension de sauvegarde en ligne.
- Cette licence d'utilisation est requise pour la sauvegarde de la boîte aux lettres unique Microsoft Exchange.
- En revanche, elle n'est pas requise pour la sauvegarde en ligne HP OpenView Network Node Manage.

Pour connaître les bases de données prises en charge, reportez-vous aux matrices de support Data Protector sous Specifications à l'adresse www.hp.com/go/dataprotector.

Tableau A-6 Extension de sauvegarde des fichiers ouverts HP OpenView Storage Data Protector

BA153AA	1 serveur
BA153BA	10 serveurs
BA154AA	5 stations de travail
BA155AA	1 serveur d'entreprise
BA152AA	CD

La licence d'utilisation de l'extension de sauvegarde des fichiers ouverts inclut la licence pour la sauvegarde de fichiers ouverts d'applications, les bases de données et les fichiers e-mail (par exemple, `.pst` - fichiers Microsoft Outlook) exécutés sur des serveurs spécifiés qui ne sont pas couverts par les matrices d'intégration et de plates-formes Data Protector.

Le CD est inclus dans le Pack Starter DVD Data Protector. Il peut également être commandé séparément via BA152AA (qui inclut le CD de sauvegarde de fichiers ouverts).

Pour connaître les configurations prises en charge, reportez-vous aux matrices de support Data Protector sous Specifications à l'adresse www.hp.com/go/dataprotector.

Tableau A-7 Extension Manager-of-Managers HP OpenView Storage Data Protector

B6956AA	pour UNIX
B6966AA	pour Windows ou Linux

La licence d'utilisation de l'extension Manager-of-Managers inclut la licence requise pour que chaque serveur de gestion (Gestionnaire de cellule) Data Protector qui s'exécute sur la plate-forme spécifiée s'intègre à un environnement Manager-of-Managers.

Vous devez disposer de cette licence pour le partage de bibliothèques de bandes entre plusieurs cellules Data Protector. Cette solution est idéale pour la gestion de sauvegarde centralisée de filiales.

Le produit B6956AA peut aussi être utilisé pour un Gestionnaire de cellule Windows. Il est toutefois plus économique d'opter pour le produit B6966AA.

Tableau A-8 Extension des opérations des supports HP OpenView Storage Data Protector

B7100AA	Niveau Entrée
B7101AA	Entreprise
B7102AA	Illimité
B7128AA	Manuels
B7129AA	CD

- Le niveau Entrée inclut la licence d'utilisation pour 2000 supports, un serveur de gestion et un nombre illimité de clients.
- Le niveau Entreprise inclut la licence d'utilisation pour 10 000 supports, un serveur de gestion et un nombre illimité de clients.
- Le niveau Illimité inclut la licence d'utilisation pour un nombre illimité de supports, un serveur de gestion et un nombre illimité de clients.

Le support désigne le nombre total de bandes consignées dans la base de données interne des opérations de support Data Protector. Vous pouvez utiliser n'importe quelle combinaison de licences des niveaux Entrée et Entreprise afin de correspondre avec le nombre total de bandes à consigner.

- Les manuels des opérations de support Data Protector sont inclus dans le lot de manuels des extensions fonctionnelles Data Protector mais peuvent être commandés séparément via B7128AA.

- Le CD-ROM des opérations de support Data Protector est inclus dans le Pack Starter DVD Data Protector mais peut également être commandé séparément via B7129AA.

Tableau A-9 Extension de sauvegarde avancée sur disque HP OpenView Storage Data Protector

B7038AA	pour 1 To
B7038BA	pour 10 To
B7038CA	pour 100 To

La licence d'utilisation de l'extension de sauvegarde avancée sur disque inclut une licence pour une capacité native correspondant au nombre de téraoctets (To) spécifiés pour l'espace de sauvegarde sur disque utilisable. L'espace de sauvegarde sur disque correspond à l'espace occupé par les sauvegardes protégées, y compris les copies et miroirs, selon la base de données interne Data Protector.

- La capacité utilisée diffère de la capacité brute dans la mesure où le surdébit RAID est exclu. Cela signifie qu'il n'est pas nécessaire de prendre en compte la configuration RAID.
- La capacité native utilisable d'une bibliothèque de bandes virtuelle correspond à l'espace occupé par les sauvegardes protégées et les miroirs et copies de sauvegarde protégés selon la base de données interne de Data Protector. Pour que la gestion des licences des bibliothèques de bandes virtuelles reste simple, un taux de compression hypothétique de 2 pour 1 est appliqué pour les bibliothèques de ce type sans supplément de prix.
- La capacité utilisée diffère de la capacité brute dans la mesure où le surdébit RAID est exclu. Cela signifie qu'il n'est pas nécessaire de prendre en compte la configuration RAID.
- L'espace de sauvegarde sur disque peut être réparti sur plusieurs baies de disques et systèmes.
- Cette extension ne requiert aucune licence d'utilisation de lecteur ou de bibliothèque. Les licences d'utilisation de lecteur et de bibliothèque sont requises pour les périphériques de fichier et non pour les sauvegardes avancées sur disque. De la même manière, la sauvegarde avancée sur disque ne peut pas être soumise aux licences de lecteur et de bibliothèque.

- Le fait que la fonctionnalité de sauvegarde sur disque est exécutée sur Windows ou Unix importe peu.
- Cette licence est requise pour la sauvegarde sur une bibliothèque de fichiers Data Protector.
- Il est possible d'utiliser cette licence pour les bibliothèques de bandes virtuelles en lieu et place des licences de lecteur et de bibliothèque. La fonctionnalité de compression intégrée des bibliothèques est transparente pour Data Protector. Un taux de compression hypothétique de 2 pour 1 est appliqué pour les bibliothèques de bandes virtuelles.

  Par exemple, une bibliothèque de bandes virtuelle avec une capacité native de 5 To peut stocker 10 To de données sauvegardées avec un taux de compression de 2 pour 1. Seules 5 licences B7038AA sont nécessaires. Vous avez la possibilité de continuer à utiliser les licences de lecteur et de bibliothèque classiques. Vous pouvez combiner plusieurs modèles de licences dans une même cellule, mais pas dans une même bibliothèque de bandes virtuelle.

REMARQUE

Dans le cas où plusieurs cellules se partagent une bibliothèque virtuelle, la licence d'utilisation Manager-of-Managers est requise pour chaque cellule afin qu'une seule licence couvre la capacité de la bibliothèque sur toutes les cellules.

Aucun supplément de prix n'est demandé pour la compression au niveau de la capacité native utilisable de la bibliothèque de fichiers Data Protector sur n'importe quel disque. La compression peut être assurée par le système d'exploitation sous-jacent ou par le système NAS (Network Attached Storage) via NFS (Network File System) ou CIFS (Common Internet File System). L'instanciation unique d'un dispositif NAS tombe également dans cette catégorie. Pour Data Protector A.05.50, un correctif est requis pour la gestion des licences portant sur la capacité native utilisable de la bibliothèque de fichiers Data Protector, sans supplément de prix pour l'instanciation unique et la compression de fournisseurs tiers.

Exemples :

— Une baie de disques de sauvegarde avec une capacité native utilisable totale de 2,5 To, entièrement utilisée pour la sauvegarde avancée sur disque, requiert 3 licences B7038AA.

— Une baie de disques de sauvegarde avec une capacité brute totale de 2,5 To, entièrement configurée dans RAID 1 (mise en miroir), a seulement une capacité native utilisable de 1,25 To et nécessite uniquement 2 licences B7038AA si elle est entièrement utilisée pour la sauvegarde avancée sur disque.

— Deux baies de disques de sauvegarde avec une capacité native utilisable totale de 2,5 To chacune, entièrement utilisées pour la sauvegarde avancée sur disque, nécessitent 5 licences B7038AA.

— Dix serveurs lame avec une capacité logique de 0,75 To chacun, entièrement utilisés pour la sauvegarde avancée sur disque, requièrent 8 licences B7038AA.

- Cette licence est également requise pour réaliser des sauvegardes complètes virtuelles ou des sauvegardes complètes synthétiques.

Tableau A-10 Extension de sauvegarde avec temps d'indisponibilité nul (ZDB) de HP OpenView Storage Data Protector

B7023CA	pour HP StorageWorks Disk Array XP, 1 To
B7023DA	pour HP StorageWorks Disk Array XP, 10 To
B7025CA	pour HP StorageWorks Enterprise Virtual Array, 1 To
B7025DA	pour HP StorageWorks Enterprise Virtual Array, 10 To
B6959CA	pour EMC Symmetrix / DMX, 1 To
B6959DA	pour EMC Symmetrix / DMX, 10 To

Le licence d'utilisation de l'extension de sauvegarde avec temps d'indisponibilité nul inclut la licence pour une capacité correspondant au nombre de téraoctets (To) pour l'espace disque utilisé sur la baie de disques spécifiée protégée par la sauvegarde avec temps d'indisponibilité nul (ZDB) et utilisant :

- HP Business Copy XP/EVA et/ou HP Continuous Access XP/EVA ou
- EMC TimeFinder et/ou EMC SRDF

La capacité d'espace disque utilisée est la capacité cumulée de tous les volumes principaux sur le type de baie de disques utilisé pour la sauvegarde avec temps d'indisponibilité nul ou pour la restauration instantanée. Le terme "principal" désigne les volumes de données de

production d'origine. Cette quantité représente la capacité totale utilisable de ces volumes, en fonction de la taille configurée pour leurs LDEV. Data Protector ne requiert pas de licences pour la capacité consommée par les volumes secondaires, les miroirs ou les snapshots utilisés pour la protection des données.

- Le surdébit RAID est exclu. Cela signifie qu'il n'est pas nécessaire de prendre en compte la configuration RAID.
- Un licence d'utilisation pour la sauvegarde en ligne (B6955BA, B6865BA) est requise pour l'exécution de la sauvegarde avec temps d'indisponibilité nul.
- La sauvegarde avec temps d'indisponibilité nul via un fournisseur matériel Microsoft Windows 2003 VSS (Volume Shadow copy Service) requiert une licence avec cette extension ZDB (par exemple, l'image instantanée du système de fichiers, Microsoft Exchange Server ou la sauvegarde Microsoft SQL Server via un fournisseur de baies de disques HP).

Tableau A-11 Extension de restauration instantanée HP OpenView Storage Data Protector

B7026CA	pour HP StorageWorks Disk Array XP, 1 To
B7026DA	pour HP StorageWorks Disk Array XP, 10 To
B7028AA	pour HP StorageWorks Enterprise Virtual Array, 1 To
B7028DA	pour HP StorageWorks Enterprise Virtual Array, 10 To

La licence d'utilisation de l'extension de restauration instantanée inclut la licence pour une capacité correspondant au nombre de téraoctets (To) spécifiés pour un espace disque utilisé ; cette licence est requise pour la restauration instantanée de la baie de disques avec la fonction Restauration instantanée. La restauration instantanée Data Protector permet de restaurer en quelques minutes des téraoctets de données à partir d'un ou de plusieurs disques de restauration, au lieu d'effectuer la restauration à partir d'une bande, ce qui pourrait demander plusieurs heures.

La capacité d'espace disque utilisée est la capacité cumulée de tous les volumes sur les types de baies de disques utilisés pour la sauvegarde avec temps d'indisponibilité nul ou pour la restauration instantanée. Le

terme "principal" désigne les volumes de données de production d'origine. Cette quantité représente la capacité totale utilisable de ces volumes, en fonction de la taille configurée pour leurs LDEV. Data Protector ne requiert pas de licences pour la capacité consommée par les volumes secondaires, les miroirs ou les snapshots utilisés pour la protection des données.

- Le surdébit RAID est exclu. Cela signifie qu'il n'est pas nécessaire de prendre en compte la configuration RAID.
- Requiert un nombre équivalent de licences d'utilisation Data Protector ZDB, qui elles-mêmes requièrent une licence d'utilisation en ligne.

Tableau A-12 Extension de la sauvegarde directe HP OpenView Storage Data Protector

B7027AA	pour HP StorageWorks Disk Array XP, 1 To
B7027DA	pour HP StorageWorks Disk Array XP, 10 To

La licence d'utilisation de l'extension de sauvegarde directe inclut la licence nécessaire pour effectuer la sauvegarde directe avec HP StorageWorks Disk Array XP, requise pour le nombre de téraoctets (To) spécifiés pour l'espace disque source utilisé nécessaire à la sauvegarde directe (sans serveur).

Requiert un nombre équivalent de licences d'utilisation Data Protector ZDB, qui elles-mêmes requièrent une licence d'utilisation en ligne.

Tableau A-13 Sauvegarde directe de HP OpenView Storage Data Protector à l'aide de NDMP

B7022BA	pour 1 To
B7022DA	pour 10 To

La licence d'utilisation de l'extension de la sauvegarde directe à l'aide de NDMP inclut la licence nécessaire pour effectuer la sauvegarde du nombre de téraoctets (To) spécifié sur 1 serveur NDMP.

Une licence est requise par téraoctet (To) d'espace disque utilisé pour chaque système de fichiers sauvegardé via NDMP (par exemple, les serveurs de fichiers Network Appliance ou EMC Celerra).

La capacité de disque utilisée correspond à la capacité totale de l'ensemble des volumes présents dans les fichiers sauvegardés via NDMP. Cette quantité représente la quantité totale utilisable de ces volumes, en fonction de la taille configurée pour leurs LDEV.

Tableau A-14 Manuels imprimés Extensions fonctionnelles HP OpenView Storage Data Protector

B6960EA	Anglais
B6960EJ	Japonais

Les manuels sont disponibles au format électronique sur les DVD, les CD et sur le site http://www.hp.com/support/manuals.

Vous pouvez commander des manuels imprimés avec les deux options suivantes : Pack Starter et Extensions fonctionnelles. Pour connaître la liste des manuels Pack Starter, reportez-vous à la section “Manuels” à la page A-20.

Les manuels imprimés Extensions fonctionnelles comportent :

- *Guide d’intégration HP OpenView Storage Data Protector pour les applications Microsoft : SQL Server, Exchange Server et Volume Shadow Copy Service*
- *Guide d’intégration HP OpenView Storage Data Protector pour Oracle et SAP*
- *Guide d’intégration HP OpenView Storage Data Protector pour les applications IBM : Informix, DB2 et Lotus Notes/Domino*
- *Guide d’intégration HP OpenView Storage Data Protector pour Sybase, Network Node Manager et le protocole NDMP (Network Data Management Protocol)*
- *Guide d’intégration HP OpenView Storage Data Protector de sauvegarde avec temps d’indisponibilité nul*
- *Guide conceptuel HP OpenView Storage Data Protector de sauvegarde avec temps d’indisponibilité nul*
- *Guide de l’administrateur HP OpenView Storage Data Protector de sauvegarde avec temps d’indisponibilité nul*
- *Guide d’intégration pour HP OpenView Service Information Portal et OpenView Reporter*

- *Guide d'intégration HP OpenView Storage Data Protector pour HP OpenView*
- *Guide d'intégration HP OpenView Storage Data Protector pour HP OpenView Operations pour UNIX*
- *Guide d'intégration HP OpenView Storage Data Protector pour HP OpenView Operations pour Windows*
- *Références, notes de publication et annonces produits OpenView Operations pour Unix*
- *Guide de l'utilisateur Data Protector Media Operations*
- *Références, notes de publication et annonces produits Data Protector Media Operations*

Editions serveur unique (SSE)

Le tableau A-15 contient les numéros de licence des Packs Starter de l'Edition serveur unique Data Protector A.06.00.

Tableau A-15 Numéros de licence des Packs Starter HP OpenView Storage Data Protector

B7020AA	DVD et licence d'utilisation SSE pour HP-UX
B7020BA	Licence d'utilisation SSE uniquement pour HP-UX
B7020DA	DVD et licence d'utilisation SSE pour Solaris
B7020CA	Licence d'utilisation SSE uniquement pour Solaris
B7030AA	DVD et licence d'utilisation SSE pour Windows
B7030BA	Licence d'utilisation SSE uniquement pour Windows
B7021AA	Migration vers le Pack Starter pour HP-UX
B7021DA	Migration vers le Pack Starter pour Solaris
B7031AA	Migration vers le Pack Starter pour Windows

Tableau A-15 Numéros de licence des Packs Starter HP OpenView Storage Data Protector

B6960MA	Kit DVD
B6960LA	Manuels Pack Starter - imprimés (anglais)
B6960LJ	Manuels Pack Starter - imprimés (japonais)
B6960LF	Manuels Pack Starter - imprimés (français)

Licence

La licence d'utilisation de l'Edition serveur unique inclut la licence qui permet de sauvegarder un serveur unique sur la plate-forme spécifiée avec un nombre illimité de stations de travail UNIX et/ou Windows et un lecteur de sauvegarde. En outre, cette édition peut gérer un changeur automatique/une bibliothèque comprenant 10 emplacements au maximum.

Migration

La licence d'utilisation de la migration inclut la licence qui permet de migrer depuis SSE ou Data Protector Express vers le Pack Starter Data Protector.

Faites migrer l'Edition serveur unique vers le Pack Starter afin de bénéficier des fonctions suivantes :

- Clients de sauvegarde supplémentaires (agents) sur toute plate-forme
- Lecteurs de sauvegarde supplémentaires
- Capacité de gérer les chargeurs automatiques/bibliothèques de plus de 10 emplacements
- Récupération après sinistre des systèmes
- Génération avancée de rapports (dans l'interface graphique utilisateur de Data Protector et via le Web)
- Prise en charge SAN (avec le serveur de gestion pour HP-UX, Solaris)
- Gestion centrée service via les intégrations avec OpenView

Pour commander la licence d'utilisation de la migration, vous devez disposer d'une licence d'utilisation pour Edition serveur unique.

Supports

Data Protector A.06.00 sera livré avec deux DVD. Si vous avez besoin de CD, il existe aussi un kit CD (B6960MB) qui contient 15 CD. Il est toutefois recommandé d'utiliser le kit DVD.

Manuels

Tous les manuels sont disponibles au format électronique sur les DVD, les CD et sur le site http://www.hp.com/support/manuals.

Vous pouvez commander des manuels imprimés avec les deux options suivantes : Pack Starter et Extensions fonctionnelles. Les manuels Pack Starter imprimés comportent :

- *Guide conceptuel HP OpenView Storage Data Protector*
- *Guide d'installation et de choix des licences HP OpenView Storage Data Protector*
- *Guide de dépannage HP OpenView Storage Data Protector*
- *Guide de récupération après sinistre HP OpenView Storage Data Protector*
- *Références, notes de publication et annonces produits HP OpenView Storage Data Protector*

REMARQUE L'Edition serveur unique pour Windows ne peut gérer que les stations de travail Windows.

Pour connaître la liste des manuels Extensions fonctionnelles, reportez-vous à la section “Manuels imprimés Extensions fonctionnelles HP OpenView Storage Data Protector” à la page A-17.

Migration de licence vers Data Protector A.06.00

La migration à partir des versions antérieures de Data Protector s'effectue comme suit :

Data Protector A.05.x

Migrez directement vers Data Protector A.06.00. Aucune migration de licence ni aucune autre sorte n'est requise. Les clients de Data Protector A.05.x sous contrat de support recevront gratuitement Data Protector A.06.00. Une fois la mise à niveau de votre environnement vers Data Protector A.06.00 effectuée, la fonctionnalité que vous utilisiez avec la version A.05.x est disponible avec Data Protector A.06.00 sans supplément de prix. Vous devez simplement acquérir de nouvelles licences si vous souhaitez vous procurer les nouvelles extensions fonctionnelles.

Présentation de la licence graphique

Figure A-2 Pack Starter pour HP-UX

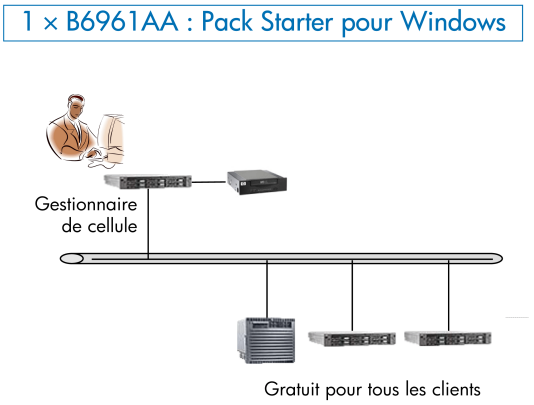


Figure A-3 Environnement mixte

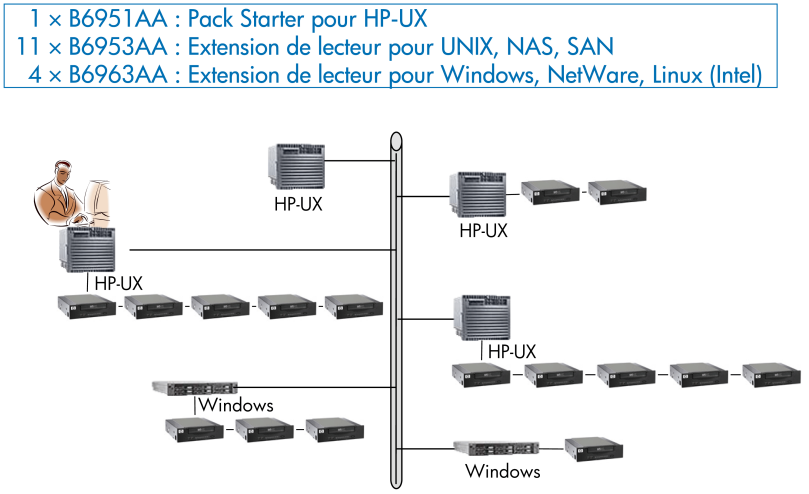


Figure A-4 **61 - 250 emplacements de bibliothèque - exemple 1**

1 × B6961AA : Pack Starter pour Windows
9 × B6963AA : Extension de lecteur pour Windows, NetWare, Linux (Intel)
4 × B6953AA : Extension de lecteur pour UNIX, NAS, SAN
1 × B6957BA : Extension pour bibliothèques 61 - 250 emplacements
1 × B6958BA : Extension pour biblio. sans limitation en nombre

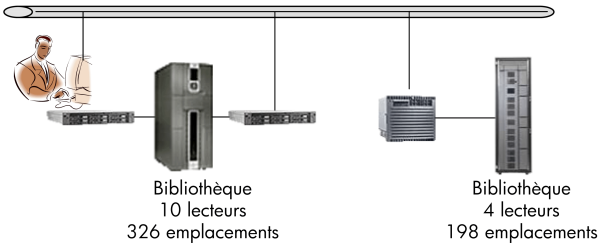


Figure A-5 **61 - 250 emplacements de bibliothèque - exemple 2**

1 × B6951AA : Pack Starter pour HP-UX
13 × B6953AA : Extension de lecteur pour UNIX, NAS, SAN
1 × B6958BA : Extension pour biblio. sans limit. en nombre
1 × B6957BA : Extension pour biblio. 61 - 250 emplacements

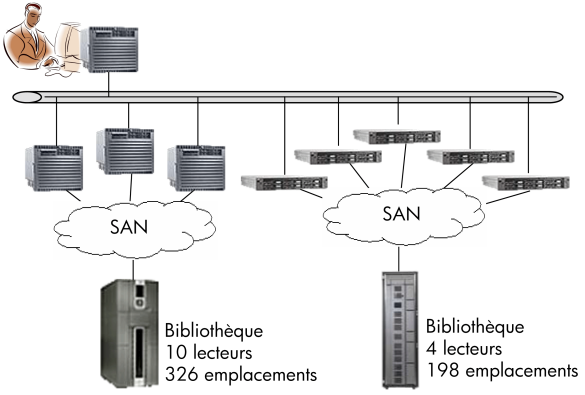


Figure A-6 Sauvegarde en ligne

1 × B6951AA : Pack Starter pour HP-UX
3 × B6953AA : Extension de lecteur pour UNIX, NAS, SAN
3 × B6963AA : Extension de lecteur pour Windows, NetWare, Linux (Intel)
4 × B6955BA : Extension pour sauvegarde en ligne UNIX
3 × B6965BA : Extension pour sauvegarde en ligne Windows

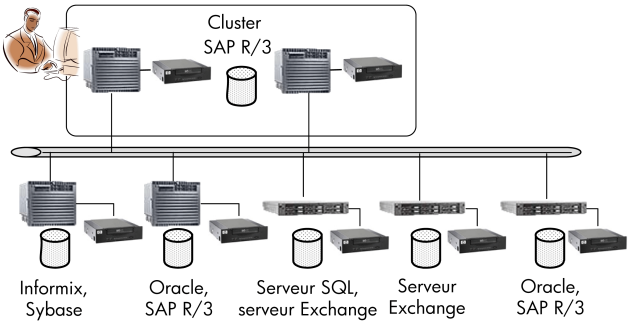


Figure A-7 Manager-of-Managers

3 × B6956AA : Extension Manager-of-Managers pour UNIX
2 × B6966AA : Extension Manager-of-Managers pour Windows
2 × B6957BA : Extension pour bibliothèques 61 - 250 emplac.

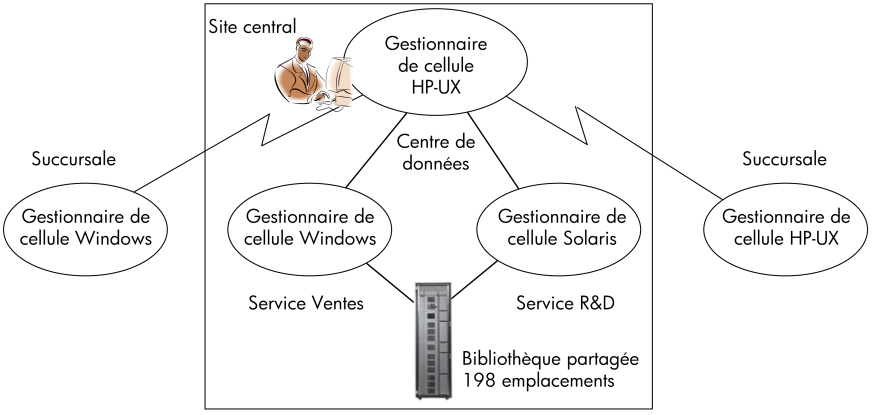


Figure A-8 **Sauvegarde avancée sur disque**

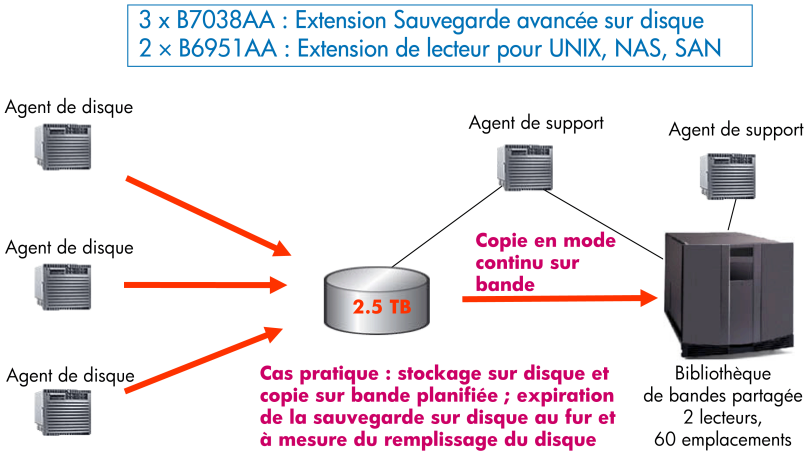
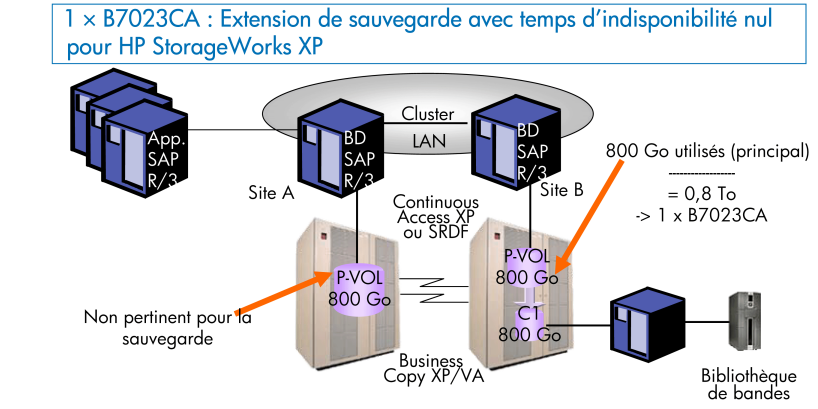
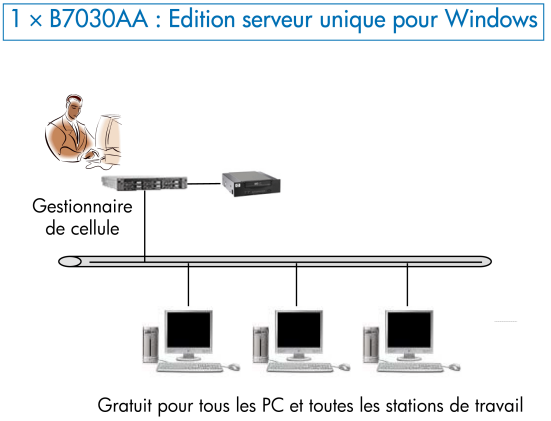


Figure A-9 **Sauvegarde avec temps d'indisponibilité nul**



Note :
- Exemple de sauvegarde avec temps d'indisponibilité nul - 800 Go LDEV
- Prise en compte des niveaux RAID non nécessaire (seuls les volumes principaux doivent être pris en compte)
- Le calcul des téraoctets (To) s'applique également à la restauration instantanée et à la sauvegarde directe

Figure A-10 Edition serveur unique



Formulaires d'attribution de licences Data Protector

Ce chapitre présente les formulaires d'attribution de licence Data Protector. Remplissez-les pour commander des mots de passe permanents à l'aide d'une des méthodes suivantes :

- Utilisez l'utilitaire HP OpenView AutoPass pour obtenir et installer les nouveaux mots de passe permanents directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations, reportez-vous à la section “Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP OpenView AutoPass” à la page 334. Cette méthode est recommandée.
- Imprimez la version électronique de ces formulaires de licence qui se trouve dans les fichiers suivants sur le système Gestionnaire de cellule et les supports de distribution :
  - HP-UX ou Solaris : `/opt/omni/doc/C/license_forms_UNIX`
  - CD-ROM Windows :

    `<Nom_disque>:Docs\license_forms.txt`

  ou utilisez les fichiers électroniques pour "copier" et "coller" votre message avant de l'adresser au *Centre de remise de mot de passe (PDC)*.
- Commandez des mots de passe permanents via le site Internet du *Centre de remise de mot de passe*, à l'adresse http://www.webware.hp.com.

IMPORTANT Assurez-vous que vous saisissez clairement les informations et que vous n'oubliez pas de renseigner les champs obligatoires.

Vous trouverez ci-après une brève description des champs des formulaires d'attribution de licence que vous devez renseigner :

Données personnelles	Ce champ contient les informations relatives au client, notamment la personne à laquelle le nouveau mot de passe doit être communiqué.
Données d'attribution de licence	Ce champ contient les informations d'attribution de licence relatives à votre cellule Data Protector.
Gestionnaire de cellule courant	Saisissez les informations requises relatives à votre Gestionnaire de cellule courant.
Nouveau Gestionnaire de cellule	Saisissez les informations requises relatives à votre nouveau Gestionnaire de cellule.
Numéro de commande	Saisissez le *numéro de commande* imprimé sur l'*attestation de droit*. Le *numéro de commande* est nécessaire pour vérifier que vous êtes autorisé à demander un mot de passe permanent.
Adresse IP	Ce champ définit le système pour lequel le *Centre de remise de mot de passe* fournira des mots de passe. Si vous souhaitez utiliser la gestion centralisée des licences (environnements MoM uniquement), ce système doit être le système Gestionnaire MoM. Si le Gestionnaire de cellule est doté de plusieurs cartes réseau, vous pouvez saisir n'importe quelle adresse IP correspondante. Il est recommandé d'utiliser l'adresse IP principale. Si vous utilisez Data Protector dans un environnement MC/Service Guard ou Microsoft Cluster, saisissez l'adresse IP de votre serveur virtuel.

	Pour plus d'informations sur les clusters, reportez-vous à l'aide en ligne.
Numéros de télécopie du *Centre de remise de mot de passe*	Pour obtenir les coordonnées, reportez-vous à l'*attestation de droit* livrée avec votre produit.
Type de licence de produit	Dans les champs situés en regard des *numéros de produit*, indiquez le nombre de licences que vous souhaitez installer sur ce Gestionnaire de cellule. Ce nombre doit être égal ou inférieur à la totalité des licences acquises avec le *numéro de commande*.

B Annexe B

Dans cette annexe

Vous trouverez dans cette annexe des informations supplémentaires relatives aux tâches qui dépassent le cadre de ce document, mais qui sont d'importance pour la procédure d'installation.

L'installation et la configuration des systèmes et périphériques pour les systèmes Windows, HP-UX et Solaris sont illustrées par des exemples.

Installation sur des systèmes HP-UX, Solaris et Linux à l'aide d'outils natifs

REMARQUE Les procédures d'installation natives sur HP-UX, Solaris et Linux ne sont documentées que si vous avez l'intention d'installer un Serveur d'installation comportant un nombre limité de packages. Il est recommandé d'installer Data Protector à l'aide de `omnisetup.sh`.

Installation d'un Gestionnaire de cellule sur un système HP-UX à l'aide de swinstall

Suivez la procédure ci-dessous pour installer le Gestionnaire de cellule UNIX sur un système HP-UX :

1. Insérez et montez le DVD-ROM d'installation UNIX et exécutez l'utilitaire `/usr/sbin/swinstall`.
2. Dans la fenêtre `Spécifier source`, sélectionnez `Chemin réseau/CDROM`, puis saisissez :
   - Sur un système PA-RISC sous HP-UX : `<Point_de_montage>/hpux_pa/DP_DEPOT/DP_A0600_UX11x.sd_depot`
   - Sur un système IA-64 sous HP-UX : `<Point_de_montage>/hpux_ia/DP_DEPOT/DP_A0600_UXia64.sd_depot`

   dans le `Chemin d'accès au dépôt source`. Cliquez ensuite sur `OK` pour ouvrir la fenêtre `Installation SD - Sélection de logiciel`.
3. Dans la liste des produits logiciels disponibles pour l'installation, vous trouverez le produit Data Protector sous la référence `B6960MA`. Cliquez deux fois sur ce dernier pour afficher le produit DATA-PROTECTOR pour UNIX. Cliquez deux fois sur ce dernier pour en afficher le contenu.

   Ce produit contient les sous-produits suivants :

   OB2-CM Logiciel du Gestionnaire de cellule

OB2-DOCS	Documentation de Data Protector comprenant les manuels Data Protector au format PDF.

4. Cliquez avec le bouton droit de la souris sur `DATA-PROTECTOR`, puis cliquez sur `Marquer pour l'installation` afin d'installer le logiciel dans son intégralité.

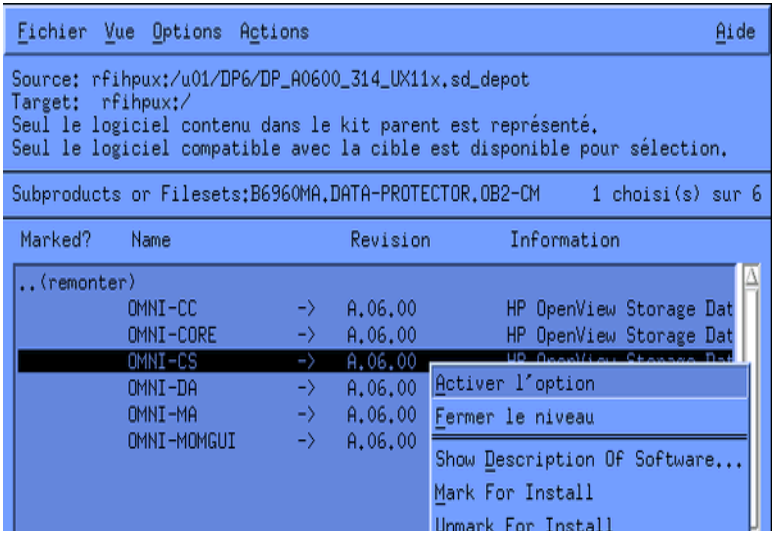
   Si vous n'avez pas besoin de tous les sous-produits, cliquez deux fois sur `DATA-PROTECTOR`, puis cliquez avec le bouton droit de la souris sur un élément de la liste. Cliquez sur `Annuler les marques pour l'installation` pour exclure le package, ou sur `Marquer pour l'installation` pour l'intégrer à l'installation.

   Assurez-vous que la valeur d'état `Marqué ?` en regard du package `OB2-CM` est réglée sur `Oui` si vous installez le Gestionnaire de cellule pour UNIX sur le système. Reportez-vous à la figure B-1.

REMARQUE Si vous utilisez des ID utilisateur de plus de 32 bits, vous devez installer le composant Interface utilisateur (OMNI-CS) à distance sur le Gestionnaire de cellule après avoir installé le composant logiciel central Gestionnaire de cellule.

5. Dans la liste `Actions`, cliquez sur `Installation (analyse)`, puis sur `OK` pour continuer. Si l'opération `Installation (analyse)` échoue et qu'un message d'erreur s'affiche, cliquez sur `Fichier journal` pour visualiser ce fichier.

Figure B-1 **Fenêtre Installation SD - Sélection de logiciel**



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

Installation d'un Gestionnaire de cellule sur des systèmes Solaris à l'aide de pkgadd

Pour installer le Gestionnaire de cellule sur un système Solaris, suivez la procédure ci-dessous :

1. Insérez le DVD-ROM d'installation UNIX.
2. Accédez au répertoire principal *<package_source>*, c'est-à-dire le répertoire contenant le fichier dépôt d'installation (dans ce cas, *<Point_de_montage>*/solaris/DP_DEPOT).

   Les packages de sous-produits suivants liés à l'installation du Gestionnaire de cellule sont inclus dans le produit :

   OB2-CORE Logiciel central Data Protector.

OB2-CC	Logiciel de la Console de cellule. Ce logiciel contient l'interface graphique utilisateur et l'interface en ligne de commande.
OB2-CS	Logiciel du Gestionnaire de cellule.
OB2 - DA	Logiciel Agent de disque. Ce logiciel est requis ; il est indispensable pour sauvegarder la base de données IDB.
et (facultatif) :	
OB2-MA	Logiciel Agent général de supports. Ce logiciel est requis si vous souhaitez connecter un périphérique de sauvegarde au Gestionnaire de cellule.
OB2-DOCS	Manuels en ligne Data Protector.

3. Utilisez la fonction `pkgadd` pour installer les packages ci-dessus.

IMPORTANT Les packages de sous-produits sous Solaris sont interdépendants. Vous devez installer ces packages en respectant l'ordre de la liste ci-dessus.

Pour installer chaque package, exécutez la commande suivante :

```
pkgadd -d DP_A0600_SUN8.pkg <nom_package>
```

4. Redémarrez les services Data Protector :

```
/opt/omni/sbin/omnisv stop
/opt/omni/sbin/omnisv start
```

REMARQUE Si vous avez installé le Gestionnaire de cellule sous Solaris 9, installez l'Agent de disque à distance sur le Gestionnaire de cellule à l'aide d'un Serveur d'installation. L'Agent de disque générique Solaris sera ainsi

remplacé par l'Agent de disque Solaris 9. Reportez-vous à la section “Installation distante de clients Data Protector” à la page 54 ou à la page man de `ob2install`.

Installation du Gestionnaire de cellule sur des systèmes Linux à l'aide de rpm

Pour installer le Gestionnaire de cellule sur un système Linux, suivez la procédure ci-dessous :

1. Insérez et montez le DVD-ROM d'installation UNIX.
2. Procédez à l'extraction des packages individuels :
   - Utilisez `rpm2cpio` (recommandé) :

     Accédez au répertoire temporaire dans lequel extraire les fichiers d'archives et exécutez la commande suivante :

     `rpm2cpio <source_package>/DP_A0600_GPLx86_64.rpm | cpio -ivd`

     Où *<source_package>* est le répertoire contenant le fichier d'archives d'installation (dans ce cas, *<Point_montage>*`/linux/DP_DEPOT`).
   - Vous pouvez également utiliser `rpm` :

     Accédez au répertoire contenant le fichier d'archives d'installation (dans ce cas, *<Point_montage>*`/linux/DP_DEPOT`, puis exécutez la commande suivante :

     `rpm -i DP_A0600_GPLx86_64.rpm`

REMARQUE

La commande `rpm -i` ci-dessus n'installe pas le logiciel. Seuls les packages RPM individuels sont copiés dans `/opt/omni`.

Toutefois, le package principal est toujours enregistré ; vous devez donc supprimer le package `OB2-CM` une fois l'installation des packages individuels terminée.

3. Accédez au répertoire dans lequel sont extraits les packages individuels :

   - Si vous avez utilisé `rpm2cpio` : `cd <répertoire_temporaire>/opt/omni`
   - Si vous avez utilisé `rpm` : `cd /opt/omni`

   Pour installer un package, exécutez la commande ci-dessous :

   ```
   rpm -i <nom_package>-A.06.00-1.x86_64.rpm
   ```

   où *<nom_package>* est le nom du package de sous-produit.

   Vous devez installer les packages suivants :

OB2-CORE	Logiciel central Data Protector.
OB2-CC	Logiciel de la Console de cellule. Ce logiciel contient l'interface de ligne de commande.
OB2-CS	Logiciel du Gestionnaire de cellule.
OB2 - DA	Logiciel Agent de disque. Ce logiciel est requis ; il est indispensable pour sauvegarder la base de données IDB.

   Vous pouvez également installer les packages suivants :

OB2-MA	Logiciel Agent général de supports. Ce logiciel est requis si vous souhaitez connecter un périphérique de sauvegarde au Gestionnaire de cellule.
OB2-DOCS	Manuels en ligne Data Protector.

IMPORTANT Les packages de sous-produits sous Linux sont interdépendants. Vous devez installer ces packages en respectant l'ordre de la liste ci-dessus.

4. Redémarrez les services Data Protector :

   ```
   /opt/omni/sbin/omnisv stop
   ```

   ```
   /opt/omni/sbin/omnisv start
   ```

5. Si vous avez utilisé `rpm` pour l'extraction du fichier d'archives RPM principal, supprimez le package `OB2-CM` :

   ```
   rpm -e OB2-CM
   ```

Installation d'un Serveur d'installation sur des systèmes HP-UX

1. Insérez et montez le DVD-ROM d'installation UNIX.
2. Dans la ligne de commande, tapez `/usr/sbin/swinstall` pour exécuter le programme d'installation.
3. Dans la fenêtre `Spécifier source`, sélectionnez `Chemin réseau/CD-ROM`, puis dans la zone `Chemin d'accès au dépôt source` saisissez :

   - Sur un système PA-RISC sous HP-UX : *<Point_de_montage>*`/hpux_pa/DP_DEPOT/DP_A0600_UX11x_IS.sd_depot`.
   - Sur un système IA-64 sous HP-UX : *<Point_de_montage>*`/hpux_ia/DP_DEPOT/DP_A0600_UXia64_IS.sd_depot`.

   Ouvrez ensuite la fenêtre `Installation SD - Sélection de logiciel`.
4. Dans cette dernière, cliquez deux fois sur `DATA-PROTECTOR` pour obtenir la liste des logiciels d'installation. Cliquez avec le bouton droit de la souris sur `OB2-IS`, puis cliquez sur `Marquer pour l'installation`.
5. Dans le menu `Actions`, cliquez sur `Installation (analyse)`. Cliquez sur `OK` pour continuer.

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

IMPORTANT

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

Installation d'un Serveur d'installation sur des systèmes Solaris à l'aide de pkgadd

Installation locale sous Solaris

Pour installer le Serveur d'installation pour UNIX sur un système Solaris, procédez comme suit :

1. Insérez le DVD-ROM d'installation UNIX.
2. Accédez au répertoire principal *<package_source>*, c'est-à-dire au répertoire contenant le fichier dépôt d'installation (dans ce cas, *<Point_montage>*/solaris/DP_DEPOT).

   Les packages de sous-produits suivants liés à l'installation du Serveur d'installation sont inclus dans le produit :

OB2-CORE	Logiciel central Data Protector. Notez que si vous installez le Serveur d'installation sur le Gestionnaire de cellule, le logiciel central est déjà installé.
OB2-C-IS	Logiciel central Serveur d'installation.
OB2-SOLUX	Paquets push de l'Agent de disque, l'Agent de support et l'interface graphique utilisateur pour les systèmes Solaris distants.
OB2-OTHUX	Paquets push de l'Agent de disque et de l'Agent de support pour systèmes UNIX non-Solaris distants.

   De plus, si vous configurez un Serveur d'installation indépendant (c'est-à-dire ne figurant pas dans le Gestionnaire de cellule) et souhaitez utiliser l'interface utilisateur :

OB2-CC	Logiciel de la Console de cellule. Ce logiciel contient l'interface graphique utilisateur et l'interface en ligne de commande.

3. Utilisez la fonction pkgadd pour installer les packages ci-dessus.

IMPORTANT Les packages de sous-produits sous Solaris sont interdépendants. Vous devez installer ces packages en respectant l'ordre de la liste ci-dessus.

Pour installer chaque package, exécutez la commande suivante :

```
pkgadd -d DP_A0600_SUN8_IS.pkg <nom_package>
```

REMARQUE La fonction `pkgadd` ne peut être exécutée que localement, pas à distance.

4. Une fois ces composants installés, utilisez `pkgadd` pour installer les paquets push de tous les packages d'intégration que vous souhaiterez installer à distance. Par exemple :

OB2-INTGP	Logiciel d'intégration central Data Protector. Ce composant est nécessaire pour installer les intégrations.
OB2-SAPP	Composant d'intégration SAP
OB2-SAPDBP	Composant d'intégration SAP DB
OB2-INFP	Composant d'intégration Informix
OB2-LOTP	Composant d'intégration Lotus Notes/Domino
OB2-SYBP	Composant d'intégration Sybase
OB2-OR8P	Composant d'intégration Oracle
OB2-DB2P	Composant d'intégration DB2
OB2-EMCP	Composant d'intégration EMC Symmetrix
OB2-SNAPP	HP StorageWorks Virtual Array
OB2-SMISAP	HP StorageWorks Enterprise Virtual Array
OB2-SSEAP	HP StorageWorks Disk Array XP
OB2-NDMPP	Logiciel Agent de support NDMP
OB2-OVP	Composant d'intégration OpenView
OB2-FRAP	Package de localisation en français
OB2-JPNP	Package de localisation en japonais

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

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

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

`/opt/omni/ -> /<préfixe>/opt/omni/`

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

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

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

REMARQUE Si vous installez le composant Interface utilisateur (interface graphique utilisateur ou interface de ligne de commande), il faut au préalable mettre à jour les variables d'environnement. Pour plus d'informations, reportez-vous à la section “Configuration des variables d'environnement” à la page 29.

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

Etape suivante

A ce stade de la procédure, les serveurs d'installation pour UNIX doivent être installés sur votre réseau. Vous devez maintenant effectuer les tâches suivantes :

1. Si vous avez configuré un Serveur d'installation indépendant (c'est-à-dire ne figurant pas dans le Gestionnaire de cellule), il faut ajouter (importer) manuellement le système dans la cellule Data Protector. Reportez-vous à la section “Importation d'un Serveur d'installation dans une cellule” à la page 199.

REMARQUE

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

2. Installez le Serveur d'installation pour Windows si vous disposez de systèmes Windows dans votre cellule Data Protector. Reportez-vous à la section “Installation d'un Serveur d'installation pour Windows” à la page 44.
3. Distribuez le logiciel aux clients. Reportez-vous à la section “Installation des clients Data Protector” à la page 50.

Installation d'un Serveur d'installation sur des systèmes Linux à l'aide de rpm

Installation locale sous Linux

Pour installer le Serveur d'installation pour UNIX sur un système Linux, procédez comme suit :

1. Insérez le DVD-ROM d'installation UNIX.
2. Procédez à l'extraction des packages individuels :
   - Utilisez `rpm2cpio` (recommandé) :

     Accédez au répertoire temporaire dans lequel extraire les fichiers d'archives et exécutez la commande suivante :

```
rpm2cpio <source_package>/DP_A0600_GPLx86_64.rpm |
cpio -ivd
```

Où *<source_package>* est le répertoire contenant le fichier d'archives d'installation (dans ce cas, *<Point_montage>*/linux/DP_DEPOT).

- Vous pouvez également utiliser `rpm` :

  Accédez au répertoire contenant le fichier d'archives d'installation (dans ce cas, *<Point_montage>*/linux/DP_DEPOT, puis exécutez la commande suivante :

  ```
  rpm -i DP_A0600_GPLx86_64_IS.rpm
  ```

REMARQUE

La commande `rpm -i` ci-dessus n'installe pas le logiciel. Seuls les packages RPM individuels sont copiés dans `/opt/omni`.

Toutefois, le package principal est toujours enregistré ; vous devez donc supprimer le package `OB2-CM` une fois l'installation des packages individuels terminée.

3. Accédez au répertoire dans lequel sont extraits les packages individuels :

   - Si vous avez utilisé `rpm2cpio` : `cd` *<répertoire_temporaire>*`/opt/omni`
   - Si vous avez utilisé `rpm` : `cd /opt/omni`

   Pour chaque package, exécutez la commande suivante :

   ```
   rpm -i <nom_package>-A.06.00-1.x86_64.rpm
   ```

   Les packages de sous-produits suivants (*<nom_package>*) liés à l'installation du Serveur d'installation sont inclus dans le produit :

OB2-CORE	Logiciel central Data Protector. Notez que si vous installez le Serveur d'installation sur le Gestionnaire de cellule, le logiciel central est déjà installé.
OB2-CORE-IS	Logiciel central Serveur d'installation.

OB2-LINUXP	Paquets push de l'Agent de disque, l'Agent de support et l'interface graphique utilisateur pour les systèmes Linux distants.
OB2-OTHUXP	Paquets push de l'Agent de disque et de l'Agent de support pour systèmes non-Linux distants.

De plus, si vous configurez un Serveur d'installation indépendant (c'est-à-dire ne figurant pas dans le Gestionnaire de cellule) et souhaitez utiliser l'interface utilisateur :

OB2-CC	Logiciel de la Console de cellule. Ce logiciel contient l'interface de ligne de commande.

4. Une fois ces composants installés, utilisez `rpm` pour installer les paquets push de tous les packages d'intégration que vous souhaiterez installer à distance. Par exemple :

OB2-INTGP	Logiciel d'intégration central Data Protector. Ce composant est nécessaire pour installer les intégrations.
OB2-SAPP	Composant d'intégration SAP
OB2-SAPDBP	Composant d'intégration SAP DB
OB2-INFP	Composant d'intégration Informix
OB2-LOTP	Composant d'intégration Lotus Notes/Domino
OB2-SYBP	Composant d'intégration Sybase
OB2-OR8P	Composant d'intégration Oracle
OB2-DB2P	Composant d'intégration DB2
OB2-EMCP	Composant d'intégration EMC Symmetrix
OB2-SNAPP	HP StorageWorks Virtual Array
OB2-SMISAP	HP StorageWorks Enterprise Virtual Array
OB2-SSEAP	HP StorageWorks Disk Array XP
OB2-NDMPP	Logiciel Agent de support NDMP
OB2-OVP	Composant d'intégration OpenView
OB2-FRAP	Package de localisation en français

OB2-JPNP Package de localisation en japonais

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

IMPORTANT

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

5. Si vous avez utilisé `rpm` pour l'extraction du fichier d'archives RPM principal, supprimez le package `OB2-CM` :

   ```
   rpm -e OB2-CM
   ```

IMPORTANT

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

`/opt/omni/ -> /<préfixe>/opt/omni/`

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

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

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

Etape suivante

A ce stade de la procédure, les serveurs d'installation pour UNIX doivent être installés sur votre réseau. Vous devez maintenant effectuer les tâches suivantes :

1. Si vous avez configuré un Serveur d'installation indépendant (c'est-à-dire ne figurant pas dans le Gestionnaire de cellule), il faut ajouter (importer) manuellement le système dans la cellule Data Protector. Reportez-vous à la section “Importation d'un Serveur d'installation dans une cellule” à la page 199.

REMARQUE

Lorsqu'un Serveur d'installation est importé, le fichier `/etc/opt/omni/server/cell/installation_servers` du Gestionnaire de cellule est mis à jour et répertorie les paquets push installés. Ce fichier peut être utilisé à partir de l'interface de ligne de commande pour

vérifier les paquets push disponibles. Pour maintenir ce fichier à jour, vous devrez exporter, puis réimporter un Serveur d'installation à chaque installation ou suppression d'un paquet push. Cette procédure est valable même dans le cas où un Serveur d'installation est installé sur le même système que le Gestionnaire de cellule.

2. Installez le Serveur d'installation pour Windows si vous disposez de systèmes Windows dans votre cellule Data Protector. Reportez-vous à la section "Installation d'un Serveur d'installation pour Windows" à la page 44.
3. Distribuez le logiciel aux clients. Reportez-vous à la section "Installation des clients Data Protector" à la page 50.

Installation des clients

Les clients ne sont pas installés pendant une installation du Gestionnaire de cellule ou du Serveur d'installation. Les clients doivent être installés soit en utilisant `omnisetup.sh`, soit en chargeant les composants d'installation à partir de l'interface graphique de Data Protector. Pour plus d'informations sur l'installation des clients, reportez-vous à la section "Installation des clients Data Protector" à la page 50.

Mise à niveau sur des systèmes HP-UX et Solaris à l'aide d'outils natifs

Mise à niveau de Data Protector sur les systèmes HP-UX à l'aide de swinstall

Une mise à niveau du Gestionnaire de cellule doit être réalisée à partir du DVD-ROM d'installation UNIX.

Si vous mettez à niveau un Gestionnaire de cellule sur lequel un Serveur d'installation est installé, vous devez d'abord effectuer la mise à niveau du Gestionnaire de cellule, puis celle du Serveur d'installation.

Les composants du client installés sur le système Gestionnaire de cellule *ne* sont *pas* mis à niveau en même temps que Gestionnaire de cellule ; ils doivent être mis à niveau en chargeant `omnisetup.sh` ou en chargeant les composants d'installation à partir du Serveur d'installation. Pour plus de détails, reportez-vous à la section "Installation locale de clients UNIX" à la page 130 ou "Installation distante de clients Data Protector" à la page 54.

Procédure de mise à niveau

Pour mettre à niveau Data Protector A.05.00, A.05.10 ou A.05.50 vers Data Protector A.06.00, à l'aide de `swinstall`, procédez comme suit :

1. Connectez-vous en tant que `root` et arrêtez les services OmniBack II/Data Protector sur le Gestionnaire de cellule en exécutant la commande `/opt/omni/sbin/omnisv -stop`.

   Tapez `ps -ef | grep omni` pour vérifier si tous les services ont bien été arrêtés. Aucun service OmniBack II/Data Protector ne doit être répertorié sur exécution de la commande `ps -ef | grep omni`.

2. Pour mettre à niveau un Gestionnaire de cellule et/ou un Serveur d'installation, suivez les procédures décrites dans la section "Installation d'un Gestionnaire de cellule sur un système HP-UX à l'aide de swinstall" à la page B-3 et/ou la section "Installation d'un Serveur d'installation sur des systèmes HP-UX" à la page B-9.

La procédure d'installation détectera automatiquement la version antérieure et mettra à niveau *uniquement les composants sélectionnés*. Si un composant installé dans la version précédente de Data Protector n'est pas sélectionné, il *n'*est *pas* mis à niveau. Par conséquent, vous devez veiller à sélectionner tous les composants à mettre à niveau.

REMARQUE

L'option `Match what target has (Sélectionner les composants de la cible)` *n'*est *pas* prise en charge si vous mettez à niveau le Gestionnaire de cellule et le Serveur d'installation sur le même système.

Mise à niveau de Data Protector sur les systèmes Solaris à l'aide de pkgadd

Pour mettre à niveau le Gestionnaire de cellule ou le Serveur d'installation de Solaris, désinstallez l'ancienne version et installez la nouvelle version du produit.

Les composants du client installés sur le système Gestionnaire de cellule *ne* sont *pas* mis à niveau en même temps que Gestionnaire de cellule ; ils doivent être mis à niveau en chargeant `omnisetup.sh` ou en chargeant les composants d'installation à partir du Serveur d'installation. Pour plus de détails, reportez-vous à la section “Installation locale de clients UNIX” à la page 130 ou “Installation distante de clients Data Protector” à la page 54.

Procédure de mise à niveau

Pour mettre à niveau Data Protector A.05.00 ou A.05.10 vers Data Protector A.05.50 à l'aide de `pkgadd`, procédez comme suit :

1. Connectez-vous en tant que `root` et arrêtez les services OmniBack II/Data Protector sur le Gestionnaire de cellule en exécutant la commande `/opt/omni/sbin/omnisv -stop`.

   Tapez `ps -ef | grep omni` pour vérifier si tous les services ont bien été arrêtés. Aucun service OmniBack II/Data Protector ne doit être répertorié sur exécution de la commande `ps -ef | grep omni`.

2. Désinstallez Data Protector à l'aide de `pkgrm`.

   Les fichiers de configuration et la base de données sont préservés durant cette procédure.

3. Exécutez la commande `pkginfo` pour vérifier que vous avez bien désinstallé l'ancienne version de Data Protector. Les anciennes versions de Data Protector ne doivent pas figurer dans la liste.

   Assurez-vous que la base de données et les fichiers de configuration sont toujours présents. Les répertoires suivants doivent toujours exister et contenir les fichiers binaires :

   - `/opt/omni`
   - `/var/opt/omni`
   - `/etc/opt/omni`

4. Si vous mettez à niveau un Gestionnaire de cellule, insérez et montez le DVD-ROM d'installation UNIX et utilisez `pkgadd` pour installer le Gestionnaire de cellule. Pour obtenir des informations détaillées sur la procédure à suivre, reportez-vous à la section “Installation d'un Gestionnaire de cellule sur des systèmes Solaris à l'aide de pkgadd” à la page B-5.

   Si vous mettez à niveau un Serveur d’installation, insérez et montez le DVD-ROM d'installation UNIX et installez le Serveur d’installation. Pour obtenir des informations détaillées sur la procédure à suivre, reportez-vous à la section “Installation d'un Serveur d’installation sur des systèmes Solaris à l'aide de pkgadd” à la page B-10.

REMARQUE

Si vous avez mis à niveau le Gestionnaire de cellule sous Solaris 9, installez l'Agent de disque à distance sur le Gestionnaire de cellule après la mise à niveau à l'aide d'un Serveur d’installation. L'Agent de disque générique Solaris sera ainsi remplacé par l'Agent de disque Solaris 9. Reportez-vous à la section “Installation distante de clients Data Protector” à la page 54 ou à la page man de `ob2install`.

Paramétrage du protocole TCP/IP sur les systèmes Windows

IMPORTANT Seule la mise en œuvre Microsoft du protocole TCP/IP est prise en charge.

Data Protector utilise le protocole TCP/IP pour les communications réseau ; celui-ci doit donc être installé et configuré sur chaque client de la cellule.

La saisie d'une commande via l'interface utilisateur Data Protector établit une connexion avec le Gestionnaire de cellule par le biais du protocole TCP/IP.

Le protocole TCP/IP est un groupe de protocoles et utilitaires reliés entre eux, utilisé pour les communications réseau. Il est constitué des protocoles TCP (Transmission Control Protocol) et IP (Internet Protocol).

Le logiciel TCP/IP est installé sur le disque dur et chaque ordinateur utilisant ce protocole doit posséder les adresses suivantes, généralement attribuées par l'administrateur réseau :

- `Adresse IP` correspondant à chaque carte réseau installée sur l'ordinateur. Il s'agit d'un numéro à 32 bits, généralement présenté sous la forme de quatre nombres séparés par des points.
- `Masque de sous-réseau` correspondant à chaque carte réseau installée sur l'ordinateur qui, associé à l'`adresse IP`, identifie l'ID réseau et l'ID hôte. Le `masque de sous-réseau` se présente dans le même format que l'`adresse IP`.
- L'adresse de la `passerelle par défaut` est requise pour la passerelle locale par défaut (routeur IP) afin de permettre l'accès Internet.

Conditions préalables

Avant d'installer le protocole TCP/IP sur un ordinateur équipé de Windows, vous devez prendre connaissance des informations suivantes :

- Différentes options de configuration sont disponibles selon le type de logiciel Windows installé sur votre ordinateur.

Un système serveur Windows peut être configuré entre autres en tant que serveur DHCP (Dynamic Host Configuration Protocol), WINS (Windows Internet Name Service) ou DNS (Domain Name System). Pour plus de détails, consultez l'aide en ligne de Windows.

- Vous pouvez configurer le protocole TCP/IP automatiquement à l'aide du DHCP à condition qu'un serveur DHCP soit installé sur votre réseau.

  Vous devez configurer le protocole TCP/IP manuellement si vous ne disposez pas d'un serveur DHCP sur votre réseau ou lorsque vous configurez le protocole TCP/IP sur le système serveur DHCP. Pour plus de détails, consultez l'aide en ligne de Windows.

- Lorsque vous configurez le protocole TCP/IP manuellement, vérifiez que vous êtes bien connecté en tant que membre du groupe Administrateurs sur l'ordinateur local. Pour éviter d'utiliser deux fois une même adresse, veillez à demander toutes les valeurs à votre administrateur réseau. Outre l'`adresse IP`, le `masque de sous-réseau` et la `passerelle par défaut` mentionnés ci-dessus, vous devez obtenir :

  ✓ le nom de votre domaine DNS et les adresses IP des serveurs DNS si vous envisagez d'utiliser des services DNS ;

  ✓ les adresses IP pour les serveurs WINS si des serveurs WINS sont présents sur votre réseau.

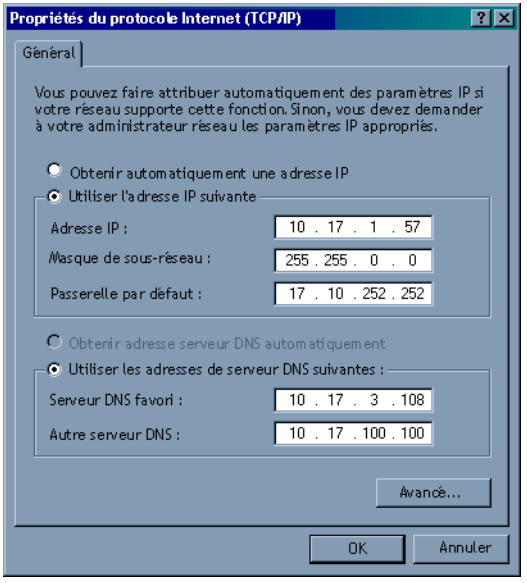
Installation et configuration du protocole TCP/IP sous Windows

Le protocole TCP/IP est installé sur les systèmes Windows au moment de l'installation du système d'exploitation.

Pour contrôler les paramètres TCP/IP actuels sur le système Windows 2000, procédez comme suit :

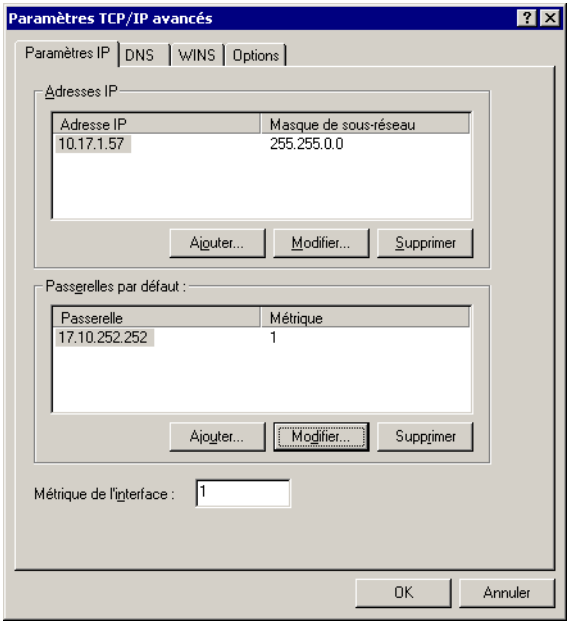
1. Dans le `Panneau de configuration` Windows, cliquez deux fois sur `Connexions réseau et accès à distance` puis sur `Connexion au réseau local`.
2. Cliquez sur `Propriétés` et double-cliquez sur `Protocole Internet (TCP/IP)`. Vous pouvez alors modifier les paramètres IP.

Figure B-2 Fenêtre Propriétés TCP/IP sous Windows



Pour modifier des paramètres avancés, cliquez sur Avancé.

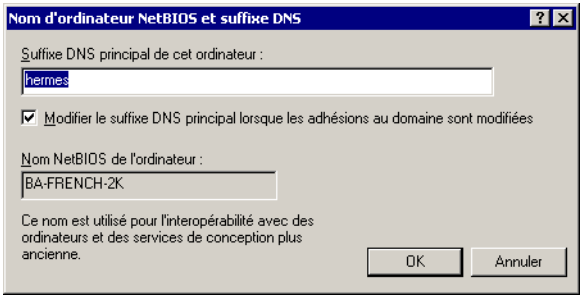
Figure B-3 Paramètres TCP/IP avancés sous Windows



Suffixe DNS

Pour configurer le suffixe DNS sur un système Windows 2000, cliquez avec le bouton droit sur l'icône `Poste de travail` du bureau, puis sélectionnez `Propriétés`, `Identification réseau`, `Propriétés`, `Autres`. Les nouveaux paramètres DNS seront pris en compte après le redémarrage du système.

Figure B-4 Suffixe DNS et nom NetBIOS de l'ordinateur sous Windows



Vérification de la configuration TCP/IP

La mise en place d'un mécanisme de résolution des noms d'hôte constitue un élément important du processus de configuration du TCP/IP.

- S'ils utilisent des fichiers d'hôtes enregistrés dans leur dossier `<%SystemRoot%>\system32\drivers\etc`, tous les systèmes de la cellule doivent pouvoir assurer la résolution de l'adresse du Gestionnaire de cellule et de toutes les machines dotées d'Agents de support et de périphériques de sauvegarde. Le Gestionnaire de cellule doit être en mesure de résoudre les noms de tous les systèmes présents dans la cellule.
- Si vous utilisez un DNS, assurez-vous que le serveur DNS local est configuré correctement et spécifié dans les paramètres IP pour chaque système de la cellule.

Une fois que vous avez installé le protocole TCP/IP, vous pouvez vérifier que sa configuration TCP/IP est correcte à l'aide des utilitaires `ping` et `ipconfig`. Si vous avez modifié les paramètres TCP/IP, redémarrez l'ordinateur.

1. Sur la ligne de commande, tapez `ipconfig /all` pour afficher les informations détaillées sur votre configuration TCP/IP et les adresses qui ont été définies pour votre carte réseau. Assurez-vous que l'adresse IP et le masque de sous-réseau sont définis correctement.
2. Tapez `ping` *`<votre_adresse_IP>`* pour confirmer l'installation et la configuration du logiciel. Par défaut, vous devez recevoir quatre paquets d'écho.
3. Tapez `ping` *`<passerelle_par_défaut>`*.

   La passerelle doit être sur votre sous-réseau. Si vous ne parvenez pas à sonder votre passerelle, vérifiez que l'adresse IP de la passerelle est correcte et que la passerelle est opérationnelle.
4. Si vous avez suivi toutes les étapes précédentes sans problème, vous pouvez maintenant tester la résolution de nom. Saisissez le nom du système dans la commande `ping` pour tester le fichier hosts et/ou le DNS.
   Si le nom de votre machine est par exemple `kesukozi` et le nom de domaine `campo.com`, vous devez taper : `ping kesukozi.campo.com`.

   Si cela ne donne pas de résultat, reportez-vous à la section “Installation et configuration du protocole TCP/IP sous Windows” à la page B-22, pour savoir comment accéder à la fenêtre `Propriétés de`

`Protocole Internet (TCP/IP)`. Vérifiez dans cette fenêtre que le nom de domaine est correct. Contrôlez également le fichier hosts et le DNS.

Assurez-vous que la résolution du nom pour le Gestionnaire de cellule et les clients fonctionne dans les deux sens :

— Sur le Gestionnaire de cellule, vous devez être en mesure de sonder (faire un ping vers) chaque client.

— Sur les clients, vous devez être en mesure de sonder (faire un ping vers) le Gestionnaire de cellule et chaque client doté d'un Agent de supports.

Notez que, lors de l'utilisation du fichier de l'hôte pour la résolution du nom, le test ci-dessus ne garantit pas le fonctionnement de la résolution du nom. Dans ce cas, vous voudrez peut-être utiliser l'**outil de vérification DNS** une fois Data Protector installé.

IMPORTANT

Si la résolution du nom, comme spécifiée ci-dessus, ne fonctionne pas, Data Protector ne peut pas être installé correctement.

Notez également que les noms de l'ordinateur Windows et de l'hôte doivent être identiques. Dans le cas contraire, Data Protector émet un avertissement.

Pour vérifier le nom d'hôte, reportez-vous à la section “Installation et configuration du protocole TCP/IP sous Windows” à la page B-22, pour savoir comment accéder à la fenêtre `Propriétés de Protocole Internet (TCP/IP)`.

5. Une fois Data Protector installé et une cellule créée, vous pouvez utiliser l'outil de vérification DNS pour vérifier que le Gestionnaire de cellule et chaque client sur lequel un Agent de support est installé résolvent correctement les connexions DNS vers tous les autres clients dans la cellule et vice versa. Pour cela, vous devez exécuter la commande `omnicheck -dns` à partir du répertoire *<répertoire_Data_Protector>*`\bin`. Les échecs des vérifications, ainsi que leur nombre sont répertoriés. Pour plus d'informations, reportez-vous à la section “Vérification des connexions DNS dans la cellule Data Protector” à la page 349.

Pour obtenir des informations détaillées sur la commande `omnicheck`, reportez-vous au document *Référence de l'interface de ligne de commande HP OpenView Storage Data Protector*.

MS Proxy

Si MS Proxy est installé, le port 5555 est occupé et les services Data Protector ne fonctionnent pas. Pour résoudre le problème, procédez comme suit :

1. Créez un fichier nommé `wspcfg.ini`, dans le répertoire *<répertoire_Data_Protector>*`\bin`.
2. Ajoutez au fichier les lignes suivantes :

```
[OmniInet]

Disable=1
```

Modification du nom du Gestionnaire de cellule

Lorsque Data Protector est installé, il utilise le nom d'hôte en vigueur pour identifier le Gestionnaire de cellule. Si vous changez le nom d'hôte de votre Gestionnaire de cellule, vous devez mettre à jour les fichiers Data Protector manuellement.

IMPORTANT

Il est nécessaire de mettre à jour les informations du client relatives au nom du Gestionnaire de cellule. Avant de modifier le nom d'hôte de votre Gestionnaire de cellule, exportez les clients à partir de la cellule. Pour connaître la procédure à suivre, reportez-vous à la section “Exportation de clients d'une cellule” à la page 204. Une fois que vous avez modifié le nom d'hôte, réimportez les clients dans la cellule. Pour connaître la procédure à suivre, reportez-vous à la section “Importation de clients dans une cellule” à la page 197.

REMARQUE

Tous les périphériques et les spécifications de sauvegarde configurés avec l'ancien nom du Gestionnaire de cellule doivent être modifiés en fonction du nouveau nom.

Sous UNIX

Avec un Gestionnaire de cellule UNIX, procédez comme suit :

1. Modifiez les entrées du nom d'hôte du Gestionnaire de cellule dans les fichiers suivants :

   ```
   /etc/opt/omni/client/cell_server
   ```

   ```
   /etc/opt/omni/server/cell/cell_info
   ```

   ```
   /etc/opt/omni/server/users/UserList
   ```

2. Vérifiez que la résolution du nom fonctionne parmi les membres d'une cellule Data Protector.

3. Changez le nom du Gestionnaire de cellule dans la base de données IDB en exécutant la commande suivante :

   ```
   /opt/omni/sbin/omnidbutil -change_cell_name
   [<ancien_hôte>]
   ```

Sous Windows

Avec un Gestionnaire de cellule Windows, procédez comme suit :

1. Modifiez les entrées du nom d'hôte du Gestionnaire de cellule dans les fichiers suivants :

   <répertoire_Data_Protector>\config\server\cell\cell_info
   <répertoire_Data_Protector>\config\server\users\userlist

2. Changez le nom du Gestionnaire de cellule dans la clé de registre suivante : \\HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBack II\Site\CellServer

Modification du numéro de port par défaut

Le service (processus) Data Protector `Inet`, lequel lance les autres processus nécessaires pour la sauvegarde et la restauration, doit utiliser le même nombre de ports sur chaque système de la cellule.

Par défaut, Data Protector utilise le numéro de port 5555. Vous devez donc afficher le fichier `/etc/services` pour les systèmes UNIX ou exécuter la commande `netstat -a` pour les systèmes Windows, pour vérifier que ce numéro de port n'est pas utilisé par un autre programme. Si le numéro de port 5555 est déjà utilisé par un autre programme, vous devez modifier cette valeur et la remplacer par un numéro de port encore inutilisé. Si le numéro de port n'est pas disponible sur les systèmes clients seulement, vous pouvez le modifier après l'installation du Gestionnaire de cellule. Si le numéro de port n'est pas disponible sur le système sur lequel installer le Gestionnaire de cellule, vous devez modifier ce numéro avant l'installation.

UNIX

Pour modifier le numéro de port sur un système UNIX, procédez comme suit :

- Avant d'installer le Gestionnaire de cellule :

  Créez le fichier `/tmp/omni_tmp/socket.dat` avec le numéro de port requis.

- Une fois le Gestionnaire de cellule installé :

  1. Editez le fichier `/etc/services`. Par défaut, ce fichier doit contenir l'entrée suivante :

     ```
     omni 5555/tcp # DATA-PROTECTOR
     ```

     Remplacez le numéro 5555 par un numéro de port inutilisé.

  2. Redémarrez le service `Inet` en tuant le processus concerné à l'aide de la commande `kill -HUP <inetd_pid>`. Pour déterminer l'ID de processus (inetd_pid), tapez `ps -ef`.

Windows

Pour modifier le numéro de port sur un système Windows, procédez comme suit :

- Avant d'installer le Gestionnaire de cellule :

  1. Dans la ligne de commande, exécutez `Regedit.exe` pour ouvrir l'`Éditeur du Registre`.
  2. Créez l'entrée de registre `InetPort` sous la clé `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Common`.

     Nom de l'entrée de registre : `InetPort`

     Type de l'entrée de registre : `REG_SZ (chaîne)`

     Valeur de l'entrée de registre : *<numéro_port>*

- Une fois le Gestionnaire de cellule installé :

  1. Dans la ligne de commande, exécutez `Regedit.exe` pour ouvrir l'`Éditeur du Registre`.
  2. Développez `HKEY_LOCAL_MACHINE`, `Software`, `Hewlett-Packard`, `OpenView`, `OmniBack II` et sélectionnez `Common`
  3. Cliquez deux fois sur `InetPort` pour ouvrir la fenêtre `Modification de la chaîne`. Dans le champ `Données de la valeur`, saisissez un numéro de port inutilisé. Procédez de même dans le sous-dossier `Parameters` du dossier `Common`.
  4. Dans le panneau de configuration Windows, accédez à `Outils d'administration, Services`, puis sélectionnez le service `Data Protector Inet` et redémarrez le service (cliquez sur l'icône `Redémarrer` dans la barre d'outils).

Préparation d'un serveur NIS

Cette procédure permet à votre serveur NIS de reconnaître votre Gestionnaire de cellule Data Protector.

Pour ajouter les informations sur Data Protector au serveur NIS, procédez comme suit :

1. Connectez-vous comme utilisateur `root` sur le serveur `NIS`.
2. Si vous gérez le fichier `/etc/services` via `NIS`, ajoutez la ligne suivante au fichier `/etc/services` :

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

   Remplacez 5555 par un autre numéro si ce port n'est pas disponible. Reportez-vous à la section “Modification du numéro de port par défaut” à la page B-30.

   Si vous gérez le fichier `/etc/inetd.conf` via `NIS`, ajoutez la ligne suivante au fichier `/etc/inetd.conf` :

   ```
   #Data Protector

   omni stream tcp nowait root /opt/omni/lbin/inet -log /var/opt/omni/log/inet.log
   ```

3. Exécutez la commande suivante pour que le serveur `NIS` lise le fichier et mette à jour la configuration.

   ```
   cd /var/yp; make
   ```

REMARQUE Dans l'environnement `NIS`, le fichier `nsswitch.conf` définit l'ordre dans lequel les différents fichiers de configuration seront utilisés. Par exemple, vous pouvez déterminer si le fichier `/etc/inetd.conf` sera utilisé sur la machine locale ou à partir du serveur `NIS`. Vous pouvez également ajouter une phrase au fichier indiquant que le fichier `nsswitch.conf` contrôle l'emplacement où les noms sont conservés. Pour plus de détails, reportez-vous aux pages du manuel correspondantes.

Si vous avez déjà installé Data Protector, vous devez préparer le serveur `NIS`, puis redémarrer le service `inet` en tuant le processus concerné ; pour cela, utilisez la commande `kill -HUP <pid>` sur chaque client constituant à la fois un client `NIS` et un client Data Protector.

Dépannage

Si le service `Data Protector Inet` ne démarre pas après l'installation de Data Protector dans votre environnement NIS, vérifiez le fichier `/etc/nsswitch.conf`.

Si vous trouvez la ligne suivante :

```
services: nis [NOTFOUND=RETURN] files
```

remplacez-la par :

```
services: nis [NOTFOUND=CONTINUE] files
```

Utilisation de pilotes de bandes et de pilotes de robots sous Windows

Data Protector prend en charge les pilotes de bandes natifs pour les lecteurs à bandes compatibles rattachés à un système Windows. Les pilotes natifs Windows chargés pour les périphériques changeurs de support (robots) ne sont pas pris en charge par Data Protector.

Dans les exemples ci-dessous, un lecteur de bandes HP 4 mm DDS est relié au système Windows. Vous devez désactiver le pilote natif chargé pour les périphériques changeurs de support si le périphérique à bandes HP 4 mm DDS est connecté à un système Windows et configuré pour être utilisé avec Data Protector. Vous trouverez dans la section ci-dessous la description des procédures correspondantes.

Pilotes de bandes

Un pilote est généralement fourni avec Windows, si le périphérique est répertorié dans la liste de compatibilité matérielle (HCL). Cette liste regroupe les périphériques supportés par Windows. Vous pouvez la trouver sur Internet, à l'adresse suivante :

http://www.microsoft.com/whdc/hcl/default.mspx

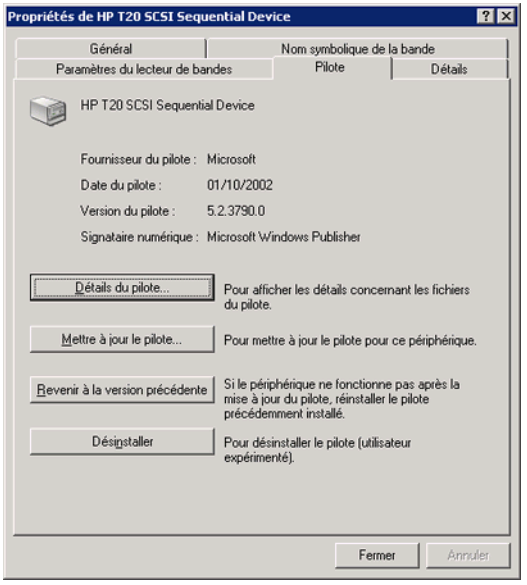
Les pilotes de périphérique sont chargés automatiquement pour tous les périphériques activés une fois que l'ordinateur a été démarré. Il est inutile de charger séparément le pilote de bandes natif, mais vous pouvez le mettre à jour.

Pour mettre à jour ou remplacer le pilote de bandes natif sur un système Windows, procédez comme suit :

1. Dans le `Panneau de configuration` Windows, cliquez deux fois sur `Outils d'administration`.
2. Dans la fenêtre `Outils d'administration`, cliquez deux fois sur `Gestion de l'ordinateur`. Cliquez sur `Gestionnaire de périphériques`.
3. Développez `Lecteurs de bande`. Pour savoir quel pilote est actuellement chargé pour le périphérique, cliquez avec le bouton droit de la souris sur le lecteur de bandes, puis sélectionnez `Propriétés`.

4. Cliquez sur l'onglet `Pilote`, puis sur `Mettre à jour le pilote`. Voir la figure B-5 à la page B-35. Suivez ensuite les instructions de l'assistant. Vous pouvez indiquer si vous souhaitez mettre à jour le pilote de bandes natif actuellement installé ou le remplacer par un autre.
5. Redémarrez le système pour appliquer les modifications.

Figure B-5 Propriétés du pilote



IMPORTANT

Si vous avez déjà configuré un périphérique pour Data Protector sans utiliser le pilote de bandes natif, vous devez renommer les fichiers de périphérique pour tous les périphériques de sauvegarde Data Protector configurés qui font référence au lecteur de bandes en question (par exemple, remplacez `scsi1:0:4:0` par `tape3:0:4:0`).

Pour plus de détails, reportez-vous à la section “Création de fichiers de périphérique (adresses SCSI) sous Windows” à la page B-38.

Pilotes de robots

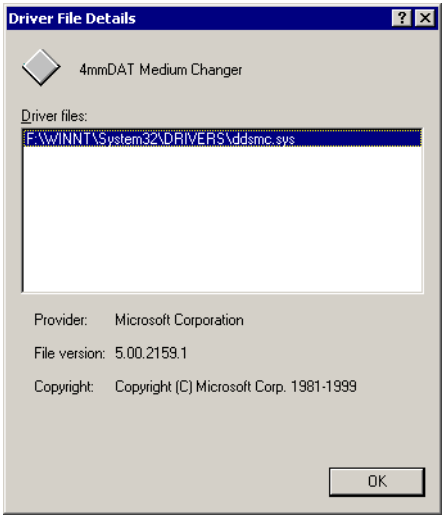
Sous Windows, les pilotes de robots sont automatiquement chargés pour les bibliothèques à bande activées. Pour pouvoir utiliser le robot de bibliothèque avec Data Protector, vous devez désactiver le pilote correspondant.

L'exemple ci-dessous présente une bibliothèque de bandes HP 1557A utilisant des bandes DDS 4 mm. Pour désactiver le pilote de robots (`ddsmc.sys`) chargé automatiquement sur un système Windows, procédez comme suit :

1. Dans le `Panneau de configuration` Windows, cliquez deux fois sur `Outils d'administration`.
2. Dans la fenêtre `Outils d'administration`, cliquez deux fois sur `Gestion de l'ordinateur`. Cliquez sur `Gestionnaire de périphériques`.
3. Dans la `zone de résultats` de la fenêtre `Gestionnaire de périphériques`, développez `Changeurs de support`.
4. Pour savoir quel pilote est actuellement chargé, cliquez avec le bouton droit de la souris sur `Changeur de support DDS 4mm`, puis sur `Propriétés`.

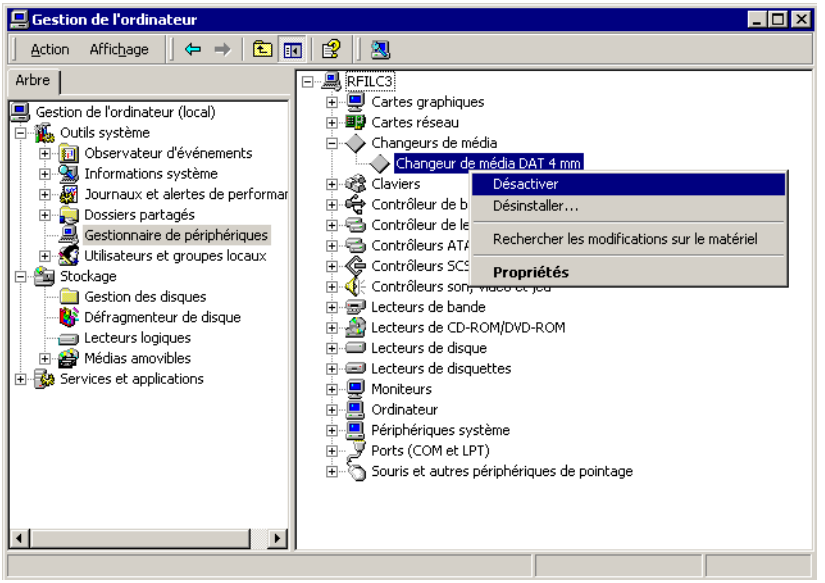
   Cliquez sur l'onglet `Pilote`, puis sur `Détails du pilote`. La fenêtre suivante s'affiche :

Figure B-6 Propriétés du changeur de support



Pour désactiver le pilote de robots natif, cliquez avec le bouton droit de la souris sur `Changeur de support DDS 4mm`, puis sélectionnez `Désactiver`.

Figure B-7 **Désactivation des pilotes de robots**



5. Redémarrez le système pour appliquer les modifications. Vous pouvez alors configurer le robot avec Data Protector.

Création de fichiers de périphérique (adresses SCSI) sous Windows

La syntaxe à utiliser pour le fichier du périphérique à bandes est différente si le pilote de bandes natif a été chargé (`tapeN:B:T:L`) ou s'il a été déchargé (`scsiP:B:T:L`) pour un lecteur de bandes.

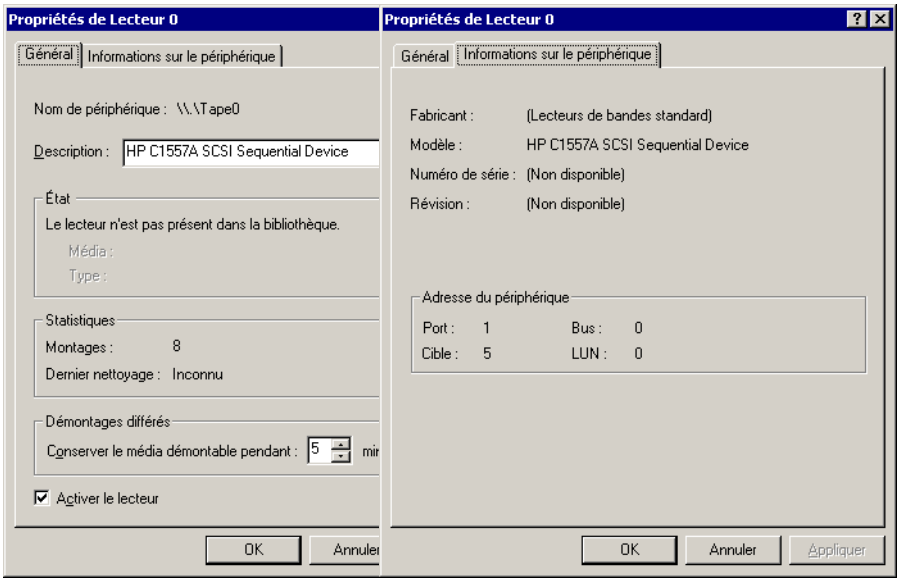
Windows avec le pilote de bandes natif

Pour créer un fichier de périphérique pour un lecteur de bande connecté à un système Windows utilisant le pilote de bandes natif, procédez comme suit :

1. Dans le `Panneau de configuration` Windows, cliquez deux fois sur `Outils d'administration`.

2. Dans la fenêtre `Outils d'administration`, cliquez deux fois sur `Gestion de l'ordinateur`. Développez `Supports amovibles`, puis `Emplacements physiques`. Cliquez avec le bouton droit de la souris sur le lecteur de bandes, puis sélectionnez `Propriétés`.
3. Si le pilote de bandes natif est chargé, le nom de fichier du périphérique s'affiche dans la page de propriétés `Général`. Sinon, vous pouvez trouver les informations utiles dans la page de propriétés `Informations sur le périphérique`. Voir la figure B-8 à la page B-39.

Figure B-8 Propriétés du lecteur de bande



Le nom de fichier pour le lecteur de bandes présenté dans la figure B-8 à la page B-39 est créé comme suit :

Pilote de bandes natif utilisé `Tape0 ou Tape0:0:5:0`

Pilote de bandes natif NON utilisé `scsii1:0:5:0`

Périphériques magnéto-optiques

Si vous connectez un périphérique magnéto-optique à un système Windows, une lettre de lecteur lui est attribuée après le réamorçage du système. Cette lettre est ensuite utilisée lorsque vous créez le fichier du périphérique. Par exemple, `E:` est le fichier de périphérique créé pour un lecteur magnéto-optique auquel la lettre de lecteur `E` a été attribuée.

Configuration de robot SCSI sous HP-UX

Sur les systèmes HP-UX, un pilote de passage SCSI est utilisé pour gérer le contrôleur SCSI *et* le périphérique de contrôle (appelé également robot ou sélectionneur) des périphériques de bibliothèque de bandes (tels que HP StorageWorks 12000e). Dans une bibliothèque, le périphérique de contrôle est utilisé pour charger/décharger les supports vers/depuis les lecteurs et importer/exporter les supports vers/depuis un périphérique de ce type.

Figure B-9 **Périphériques SCSI contrôlés**

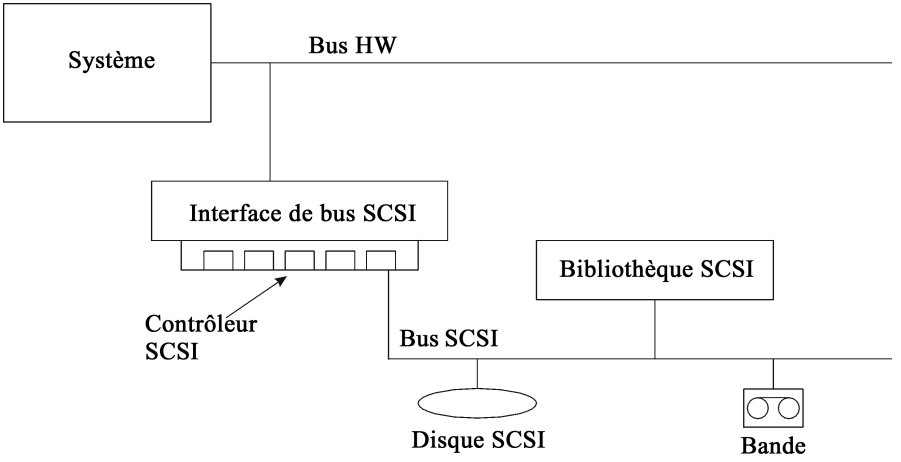
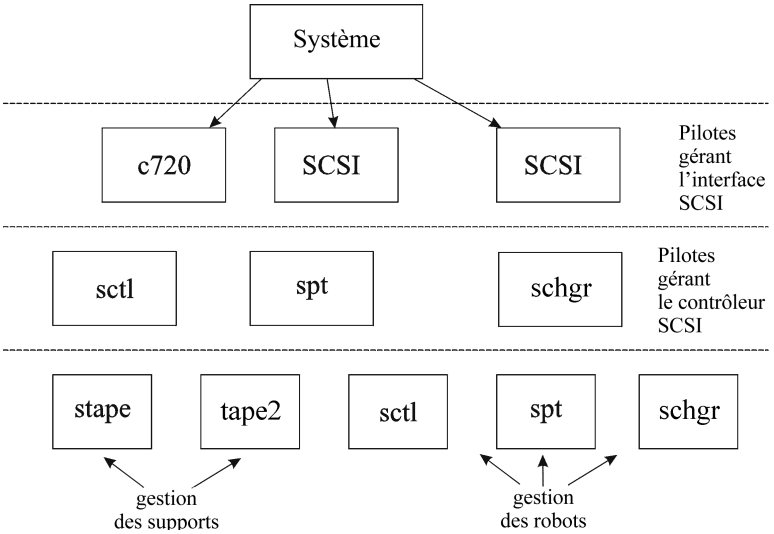


Figure B-10 Gestion des périphériques



Le type de pilote de robot SCSI utilisé dépend du matériel. Les systèmes équipés du bus `GSC/HSC` ou `PCI` sont dotés du pilote de changeur automatique SCSI nommé `schgr`, tandis que les systèmes équipés du bus `EISA` possèdent le pilote de passage SCSI nommé `sctl`, lequel est déjà intégré dans le noyau. En revanche, le pilote de passage SCSI utilisé sur les serveurs HP avec un bus NIO est nommé `spt`. Il est installé sur le système sans être intégré par défaut au noyau.

Si le pilote de robot SCSI n'a pas encore été relié à votre noyau actuel, vous devez l'ajouter manuellement et l'attribuer au robot des bibliothèques de bandes connectées.

Pour ajouter *manuellement* le pilote de robot SCSI au noyau et en recréer un autre manuellement, suivez la procédure ci-dessous.

CONSEIL

Sur la plate-forme HP-UX, vous pouvez également créer le noyau à l'aide de l'utilitaire *HP System Administration Manager (SAM)*. Reportez-vous à la section “Installation de clients HP-UX” à la page 74 du Chapitre 2.

Utilisez la commande `/opt/omni/sbin/ioscan -f` pour savoir si le pilote de robot SCSI est attribué à la bibliothèque que vous souhaitez configurer.

Figure B-11 Etat du pilote de passage SCSI (sctl)

```
root@superhik$ ioscan -f
Class       I  H/W Path    Driver      S/W State H/W Type  Description
=============================================================================
bc          0              root        CLAIMED   BUS_NEXUS
bc          1  8           ccio        CLAIMED   BUS_NEXUS I/O Adapter
unknown    -1  8/0                     CLAIMED   DEVICE    GSC-to-PCI Bus Bridge
ext_bus     0  8/12        c720        CLAIMED   INTERFACE GSC Fast/Wide SCSI Interfac
e
target      0  8/12.0      tgt         CLAIMED   DEVICE
disk        0  8/12.0.0    sdisk       CLAIMED   DEVICE    SEAGATE ST19171W
target      1  8/12.1      tgt         CLAIMED   DEVICE
tape        5  8/12.1.0    stape       CLAIMED   DEVICE    QUANTUM DLT7000
target      2  8/12.2      tgt         CLAIMED   DEVICE
ctl         0  8/12.2.0    sctl        CLAIMED   DEVICE    EXABYTE EXB-210
target      3  8/12.7      tgt         CLAIMED   DEVICE
ctl         0  8/12.7.0    sctl        CLAIMED   DEVICE    Initiator
ba          0  8/16        bus_adapter CLAIMED   BUS_NEXUS Core I/O Adapter
ext_bus     2  8/16/0      CentIf      CLAIMED   INTERFACE Built-in Parallel Interface
audio       0  8/16/1      audio       CLAIMED   INTERFACE Built-in Audio
tty         0  8/16/4      asio0       CLAIMED   INTERFACE Built-in RS-232C
ext_bus     1  8/16/5      c720        CLAIMED   INTERFACE Built-in SCSI
target      4  8/16/5.2    tgt         CLAIMED   DEVICE
disk        2  8/16/5.2.0  sdisk       CLAIMED   DEVICE    TOSHIBA CD-ROM XM-5401TA
target      7  8/16/5.3    tgt         NO_HW     DEVICE
tape        3  8/16/5.3.0  stape       NO_HW     DEVICE    SONY     SDX-300C
target      6  8/16/5.5    tgt         NO_HW     DEVICE
tape        0  8/16/5.5.0  stape       NO_HW     DEVICE    SONY     SDX-300C
target      5  8/16/5.7    tgt         CLAIMED   DEVICE
```

La figure B-11 à la page B-43 vous indique le pilote de passage SCSI `sctl` affecté au périphérique de contrôle du périphérique à bandes Exabyte. Le chemin matériel correspondant (H/W Path) est `8/12.2.0`. (SCSI=2, LUN=0).

Un lecteur de bandes est connecté au même bus SCSI, mais le pilote qui le contrôle est `stape`. Le chemin de matériel correspondant (H/W Path) est `8/12.1.0`. (SCSI=0, LUN=0)

IMPORTANT

L'adresse SCSI 7 est toujours utilisée par les contrôleurs SCSI, bien que la ligne correspondante n'apparaisse pas forcément dans les résultats de la commande `ioscan -f`. Dans cet exemple, le contrôleur est géré par `sctl`.

Figure B-12 Etat du pilote de passage SCSI - spt

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
=============================================================
bc          0             root      CLAIMED   BUS_NEXUS
ext_bus     0  52         scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1       target    CLAIMED   DEVICE
disk        4  52.1.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2       target    CLAIMED   DEVICE
disk        0  52.2.0     disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4       target    CLAIMED   DEVICE
tape        0  52.4.0     tape2     CLAIMED   DEVICE    HP       C1533A
spt         1  52.4.1     spt       CLAIMED   DEVICE    HP       C1553A
target      6  52.5       target    CLAIMED   DEVICE
disk        5  52.5.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6       target    CLAIMED   DEVICE
disk        1  52.6.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56         lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0       mux4      CLAIMED   INTERFACE
lan         0  56.1       lan3      CLAIMED   INTERFACE
lantty      0  56.2       lantty0   CLAIMED   INTERFACE
processor   0  62         processor CLAIMED   PROCESSOR Processor
memory      0  63         memory    CLAIMED   MEMORY    Memory
#
```

La figure B-12 à la page B-44 donne un exemple de périphérique à bandes connecté, avec un robot contrôlé par le pilote de passage SCSI `spt`. Le périphérique en question est un périphérique de bibliothèque de bandes HP StorageWorks 12000e qui utilise l'adresse SCSI 4 et est connecté au bus SCSI avec le chemin matériel 52. Le chemin matériel correspondant est 52.4.1. Le robot est correctement affecté au pilote de passage SCSI `spt`.

Si le pilote `sctl`, `spt` ou `schgr` n'est pas affecté au robot, vous devez ajouter le chemin matériel du robot à l'instruction du pilote dans le fichier `system`, puis recréer le noyau. Pour cela, suivez la procédure ci-dessous.

Pour ajouter *manuellement* un pilote de robot SCSI au noyau, l'affecter au robot, puis recréer manuellement un nouveau noyau, procédez comme suit :

1. Connectez-vous comme utilisateur *root*, puis basculez vers le répertoire build :

   ```
   cd /stand/build
   ```

2. Créez un fichier système à partir du kernel existant :

   ```
   /usr/lbin/sysadm/system_prep -s system
   ```

3. Vérifiez quel pilote de robot SCSI est déjà intégré au noyau en cours. A partir du répertoire `/stand`, tapez la commande suivante :

   `grep <pilote de robot SCSI> system`

   où *<pilote de robot SCSI>* peut être `spt`, `sctl` ou `schgr`. Le système affiche alors la ligne correspondante si le pilote est déjà intégré au noyau en cours.

4. Utilisez un éditeur pour ajouter une instruction de pilote :

   `driver <chemin matériel> spt`

   au fichier `/stand/build/system`, où *<chemin matériel>* correspond au chemin matériel complet du périphérique.

   Pour la bibliothèque de bandes HP StorageWorks 12000e de l'exemple précédent, vous auriez saisi :

   ```
   driver 52.4.1 spt
   ```

   Si plusieurs bibliothèques sont connectées au même système, vous devez ajouter une ligne de pilote pour chaque robot de bibliothèque, avec le chemin matériel approprié.

   Lorsque vous configurez le pilote `schgr`, ajoutez la ligne suivante à l'instruction de pilote :

   ```
   schgr
   ```

5. Tapez la commande `mk_kernel -s./system` pour construire un nouveau noyau.

6. Enregistrez l'ancien fichier system sous un autre nom et renommez le nouveau fichier system avec le nom initial pour qu'il devienne le fichier en vigueur :

   ```
   mv /stand/system /stand/system.prev
   mv /stand/build/system /stand/system
   ```

7. Enregistrez l'ancien noyau sous un autre nom et renommez le nouveau noyau avec le nom initial pour qu'il devienne le noyau en vigueur :

   ```
   mv /stand/vmunix /stand/vmunix.prev
   mv /stand/vmunix_test /stand/vmunix
   ```

8. Réamorcez le système à partir du nouveau noyau en tapant la commande suivante :

   ```
   shutdown -r 0
   ```

9. Après la réinitialisation du système, vérifiez vos modifications à l'aide de la commande `/usr/sbin/ioscan -f`.

Création de fichiers de périphérique sous HP-UX

Conditions préalables

Avant de créer un fichier de périphérique, le périphérique de sauvegarde doit être connecté au système. Utilisez la commande `/usr/sbin/ioscan -f` pour vérifier que le périphérique est correctement connecté. Utilisez la commande `/usr/sbin/infs -e` pour créer automatiquement les fichiers de périphérique pour certains périphériques de sauvegarde.

Si les fichiers de périphérique correspondant à un périphérique de sauvegarde particulier n'ont pas été créés lors de l'initialisation du système (processus d'amorçage) ou après exécution de la commande `infs -e`, vous devez les créer manuellement. Cela concerne notamment les fichiers de périphérique requis pour la gestion du périphérique de contrôle de bibliothèque (robot de bibliothèque).

Prenons l'exemple de la création d'un fichier de périphérique pour le robot du périphérique de bibliothèque HP StorageWorks 12000e connecté à un système HP-UX 11.00. Le fichier de périphérique correspondant au lecteur de bandes a déjà été créé automatiquement après la réinitialisation du système, tandis que le fichier de périphérique correspondant au périphérique de contrôle doit être créé manuellement.

La figure B-12 à la page B-44 vous présente les résultats de la commande `ioscan -f` sur le système HP-UX sélectionné.

Figure B-13 Liste des périphériques connectés

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
=============================================================
bc          0             root      CLAIMED   BUS_NEXUS
ext_bus     0  52         scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1       target    CLAIMED   DEVICE
disk        4  52.1.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2       target    CLAIMED   DEVICE
disk        0  52.2.0     disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4       target    CLAIMED   DEVICE
tape        0  52.4.0     tape2     CLAIMED   DEVICE    HP       C1533A
spt         1  52.4.1     spt       CLAIMED   DEVICE    HP       C1553A
target      6  52.5       target    CLAIMED   DEVICE
disk        5  52.5.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6       target    CLAIMED   DEVICE
disk        1  52.6.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56         lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0       mux4      CLAIMED   INTERFACE
lan         0  56.1       lan3      CLAIMED   INTERFACE
lantty      0  56.2       lantty0   CLAIMED   INTERFACE
processor   0  62         processor CLAIMED   PROCESSOR Processor
memory      0  63         memory    CLAIMED   MEMORY    Memory
#
```

L'interface du bus SCSI est contrôlée par le pilote système `scsi1`. Il s'agit d'une interface `SCSI NIO`. Pour accéder au robot de bibliothèque sur le bus `SCSI NIO`, il faut utiliser le pilote de passage SCSI `spt` qui est déjà installé et affecté au robot du périphérique à bandes HP StorageWorks 12000e, lequel utilise le chemin matériel `52.4.1`.

REMARQUE Si vous n'utilisez pas une interface de bus basée sur `SCSI NIO`, le pilote `spt` n'est pas nécessaire, mais le pilote `sctl` est utilisé à sa place.

Pour créer un fichier de périphérique, vous devez connaître le *numéro majeur* du pilote de passage SCSI et le *numéro mineur*, qui ne dépend pas du pilote de passage SCSI que vous utilisez.

Pour obtenir le *numéro majeur* correspondant au `spt`, exécutez la commande suivante :

```
lsdev -d spt
```

Dans notre exemple (voir figure B-13 à la page B-47), la commande renvoie le *numéro majeur* `75`.

Pour obtenir le *numéro majeur* correspondant au `sctl`, exécutez la commande suivante :

```
lsdev -d sctl
```

Dans notre exemple, la commande renvoie le *numéro majeur* `203`.

Le *numéro mineur*, indépendamment du pilote de passage SCSI utilisé, se présente sous la forme suivante :

`0xIITL00`

`II` -> *Numéro d'instance* de l'interface du bus SCSI (PAS celui du périphérique) consigné dans les résultats de la commande `ioscan -f` et se trouvant dans la deuxième colonne libellée `I`. Dans cet exemple, le numéro d'instance est `0`, il faut donc entrer deux chiffres hexadécimaux : 00.

`T` -> L'adresse SCSI du robot de bibliothèque. Dans cet exemple, l'adresse SCSI est `4` ; il faut donc entrer `4`.

`L` -> Numéro LUN du robot de bibliothèque. Dans cet exemple, le numéro LUN est `1` ; il faut donc entrer `1`.

`00` -> Deux zéros hexadécimaux.

Création du fichier de périphérique

Pour créer le fichier de périphérique, utilisez la commande suivante :

`mknod /dev/spt/<nom_fichier_périphérique> c Num_majeur Num_mineur`

Les fichiers de périphérique `spt` se trouvent généralement dans le répertoire `/dev/spt` ou `/dev/scsi`. Dans cet exemple, nous appelons le fichier du périphérique de contrôle `/dev/spt/SS12000e`.

Par conséquent, la commande complète à utiliser pour la création d'un fichier de périphérique nommé `SS12000e` dans le répertoire `/dev/spt` est la suivante :

```
mknod /dev/spt/SS12000e c 75 0x004100
```

Pour créer un fichier de périphérique correspondant à `sctl`, nommé SS12000e et situé dans le répertoire `/dev/scsi`, la commande complète à utiliser est la suivante :

```
mknod /dev/scsi/SS12000e c 203 0x004100
```

Configuration des paramètres du contrôleur SCSI

Data Protector permet de modifier la taille de bloc du périphérique. Pour ce faire, vous devez procéder à une configuration supplémentaire de certains contrôleurs SCSI : pour permettre l'écriture de tailles de bloc supérieures à 64 Ko, la configuration des paramètres de certains contrôleurs SCSI doit être modifiée.

Pour définir les paramètres de contrôleur SCSI sur un système Windows, vous devez modifier la valeur de registre des contrôleurs SCSI Adaptec et de certains contrôleurs dotés de chipsets Adaptec :

1. Définissez la valeur de registre suivante :
   `\\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aic78xx\Parameters\Device0\MaximumSGList`
2. Saisissez une valeur `DWORD` contenant le nombre de blocs de 4 Ko augmenté de un.

   `MaximumSGList = (OBBlockSize en Ko / 4) + 1`

   Par exemple, pour permettre l'écriture de blocs dont la taille peut atteindre 260 Ko, `MaximumSGList` doit être au moins égal à `(260 / 4) + 1 = 66`.
3. Redémarrez le système.

REMARQUE La valeur de registre définit la limite supérieure de la taille de bloc. Pour configurer la taille de bloc en cours pour un périphérique, vous devez utiliser l'interface graphique utilisateur de Data Protector.

Recherche des adresses SCSI non utilisées sous HP-UX

Le contrôle et l'accès à un périphérique de sauvegarde connecté à un système HP-UX se font via un fichier de périphérique qui doit se trouver sur chaque périphérique physique. Avant de créer le fichier de périphérique, vous devez rechercher quelles adresses SCSI (ports) restent inutilisées et disponibles pour un nouveau périphérique.

Sous HP-UX, utilisez la commande système `/usr/sbin/ioscan -f` pour afficher la liste des adresses SCSI déjà occupées. Les adresses qui ne figurent pas dans la liste obtenue par la commande `/usr/sbin/ioscan -f` sont par conséquent inutilisées.

La figure B-14 à la page B-50 présente les résultats de la commande `/usr/sbin/ioscan -f` sur un système HP-UX 11.x.

Figure B-14 Résultats de `ioscan -f` sur un système HP-UX :

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
=============================================================
bc          0           root      CLAIMED   BUS_NEXUS
ext_bus     0  52        scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1      target    CLAIMED   DEVICE
disk        4  52.1.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2      target    CLAIMED   DEVICE
disk        0  52.2.0    disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4      target    CLAIMED   DEVICE
tape        0  52.4.0    tape2     CLAIMED   DEVICE    HP      C1533A
spt         1  52.4.1    spt       CLAIMED   DEVICE    HP      C1553A
target      6  52.5      target    CLAIMED   DEVICE
disk        5  52.5.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6      target    CLAIMED   DEVICE
disk        1  52.6.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56        lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0      mux4      CLAIMED   INTERFACE
lan         0  56.1      lan3      CLAIMED   INTERFACE
lantty      0  56.2      lantty0   CLAIMED   INTERFACE
processor   0  62        processor CLAIMED   PROCESSOR Processor
memory      0  63        memory    CLAIMED   MEMORY    Memory
#
```

Seules la troisième `(chemin H/W)` et la cinquième `(état S/W)` colonnes sont utiles pour déterminer les adresses SCSI disponibles. Un format de `(chemin H/W)` démembré se présenterait sous la forme suivante :

<Chemin_H/W_bus_SCSI>.<adresse_SCSI>.<numéro_LUN>

Dans ce cas particulier, il n'y a qu'un bus SCSI, qui utilise le chemin H/W 52. Pour ce bus, vous pouvez utiliser les adresses SCSI `0` et 3, puisqu'elles ne figurent pas dans la liste.

La figure B-14 à la page B-50 vous indique quelles sont les adresses du bus SCSI sélectionné qui sont déjà occupées :

- L'adresse SCSI 1 est occupée par un disque SCSI.
- L'adresse SCSI 2 est occupée par un CD-ROM.
- L'adresse SCSI 4, LUN 0, est occupée par un lecteur de bandes.
- L'adresse SCSI 4, LUN 1, est occupée par la bibliothèque de bandes.
- L'adresse SCSI 5 est occupée par un disque SCSI.
- L'adresse SCSI 6 est occupée par un disque SCSI.
- L'adresse SCSI 7 est occupée par un contrôleur SCSI.

REMARQUE Bien que l'adresse SCSI numéro 7 *ne* figure *pas* dans la liste, elle est occupée par défaut par le contrôleur SCSI.

Pour tous les périphériques, la valeur `Etat S/W` est définie à `UTILISE` (CLAIMED) et la valeur `Type H/W` est définie à `PERIPHERIQUE` (H/W DEVICE) ce qui signifie que les périphériques sont actuellement connectés. Si une valeur `INUTILISE` (UNCLAIMED) figurait dans la colonne `Etat S/W` ou `AUCUN PERIPHERIQUE` (NO H/W) dans la colonne `Type H/W`, cela signifierait que le système ne peut pas accéder au périphérique.

L'adresse SCSI 4 est demandée par la bibliothèque de bandes, dotée du lecteur de bandes avec le LUN 0 et du robot avec le LUN 1. Le lecteur est contrôlé par le pilote `tape2` et le robot par le pilote de passage SCSI `spt`. Dans la description, vous pouvez constater que le périphérique est une bibliothèque HP StorageWorks 12000e ; celle-ci est facilement reconnaissable parmi les autres bibliothèques SCSI car elle utilise la même adresse SCSI pour le lecteur de bandes et le robot, mais avec des LUN différents.

Tout le bus SCSI est contrôlé par le module d'interface `scsi1`.

Recherche des ID SCSI cibles inutilisés sous Solaris

L'accès et le contrôle d'un périphérique de sauvegarde connecté à un système Solaris se fait via un fichier de périphérique. Ce fichier de périphérique est automatiquement créé par le système d'exploitation Solaris dans le répertoire `/dev/rmt`, au moment de la connexion du périphérique de sauvegarde et de la mise sous tension du système client et du périphérique de sauvegarde.

Toutefois, avant de connecter le périphérique de sauvegarde, les adresses SCSI disponibles doivent être vérifiées et l'adresse du périphérique de sauvegarde doit être établie sur une adresse non encore allouée.

Pour répertorier les adresses SCSI disponibles sur un système Solaris, procédez comme suit :

1. Arrêtez le système en appuyant sur `Stop` et `A`.
2. A l'invite `ok`, exécutez la commande `probe-scsi-all` :

   ```
   probe-scsi-all
   ```

   Le système peut vous demander de lancer la commande `reset-all` avant d'exécuter la commande `probe-scsi-all`.
3. Pour revenir au fonctionnement normal, tapez `go` à l'invite `ok` :

   ```
   go
   ```

Après avoir répertorié les adresses disponibles et choisi celle que vous souhaitez utiliser pour votre périphérique de sauvegarde, vous devez mettre à jour les fichiers de configuration appropriés avant de connecter et de démarrer le périphérique. Reportez-vous à la section suivante pour obtenir des instructions sur la mise à jour des fichiers de configuration.

Mise à jour de la configuration des périphériques et pilotes sur un système Solaris

Mise à jour des fichiers de configuration

Les fichiers de configuration suivants servent à la configuration du périphérique et du lecteur. Ils doivent être vérifiés, et modifiés le cas échéant, avant que les périphériques connectés ne puissent être utilisés :

- `st.conf`
- `sst.conf`

st.conf : Tous les périphériques

Ce fichier est requis sur tout client Solaris Data Protector auquel est connecté un périphérique à bandes. Il doit contenir des informations sur le périphérique et une ou plusieurs adresses SCSI pour chaque périphérique de sauvegarde connecté au client. Une seule entrée SCSI est requise pour un périphérique à lecteur unique, tandis qu'il en faut plusieurs pour un périphérique de bibliothèque multi-lecteurs.

1. Vérifiez quelles sont les adresses SCSI inutilisées sur le client, tel que le décrit la section précédente, et choisissez une adresse pour le périphérique à connecter.
2. Définissez les adresses SCSI choisies sur le périphérique de sauvegarde.
3. Eteignez le système client.
4. Connectez le périphérique de sauvegarde.
5. Remettez le périphérique sous tension, puis le système client.
6. Arrêtez le système en appuyant sur `Stop` et `A`.
7. A l'invite `ok`, tapez la commande `probe-scsi-all` :

   ```
   probe-scsi-all
   ```

   Cela permet de fournir des informations sur les périphériques SCSI connectés, notamment la chaîne d'identification correcte du périphérique de sauvegarde nouvellement connecté.

8. Revenez en fonctionnement normal :

   ```
   go
   ```

9. Modifiez le fichier `/kernel/drv/st.conf`. Ce fichier est utilisé par le pilote (bande SCSI) `st` de Solaris. Il contient une liste des périphériques officiellement pris en charge par Solaris, ainsi qu'un ensemble de saisies de configuration pour des périphériques tiers. Si vous utilisez un périphérique non pris en charge, il devrait être possible de le connecter et de l'utiliser sans configuration supplémentaire. Sinon, vous pouvez ajouter les types d'entrée suivants dans le fichier `st.conf` :

   - Une entrée de liste de configuration de bande (plus une définition de variable de données de bandes). Des exemples d'entrées, accompagnés de commentaires, sont fournis dans le fichier. Si l'un d'eux vous convient, vous pouvez l'utiliser ; vous pouvez également les modifier pour les adapter à vos besoins.

     L'entrée doit venir avant la première entrée `name=` du fichier et le format requis est le suivant :

     tape-config-list= "*<périphérique à bandes>*", "*<nom de référence du périphérique à bandes>*", "*<données de bandes>*";

     où :

     <périphérique à bandes> Chaîne d'identification du fournisseur et du produit pour le périphérique à bandes. Celui-ci doit être correctement spécifié, en conformité avec la documentation du constructeur du périphérique.

     <nom de référence du périphérique à bandes> Nom que vous choisissez, par lequel le système identifiera le périphérique à bandes. Ce nom ne modifie pas l'identification du produit mais, lorsque le système démarre, c'est le nom de référence qui s'affiche la liste des périphériques reconnus par le système.

     <données de bandes> Variable qui fait référence à des éléments supplémentaires de configuration du périphérique à bandes. La définition de la variable doit elle aussi être indiquée

correctement, conformément aux dispositions de la documentation du constructeur du périphérique.

Par exemple :

```
tape-config-list= ""Quantum DLT4000", "Quantum DLT4000",
"DLT-data";

DLT-data = 1,0x38,0,0xD639,4,0x80,0x81,0x82,0x83,2;
```

Le deuxième paramètre, `0x38`, désigne le type de bande DLT comme "autre lecteur SCSI". La valeur spécifiée ici doit être définie dans `/usr/include/sys/mtio.h`.

REMARQUE Assurez-vous que la dernière entrée de la ligne tape-config-list se termine par un point-virgule (;).

- Pour les périphériques multi-lecteurs, ciblez les saisies comme suit :

```
name="st" class="scsi"
target=X lun=Y;
```

où :

X	correspond au port SCSI affecté au lecteur de données (ou mécanisme du robot).
Y	est la valeur de l'unité logique.

Par exemple :

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

name="st" class="scsi"
target=2 lun=0
```

Normalement, les entrées cibles sont requises dans le fichier `st.conf` pour les lecteurs uniquement, et non pour le mécanisme du robot, qui est présent sur une autre cible. Elles sont généralement fournies dans le fichier `sst.conf` (voir ci-dessous). En revanche, il existe certains périphériques, tel que le HP StorageWorks 24x6, qui traitent le mécanisme du robot de la

même manière qu'un autre lecteur. Dans ce cas, deux entrées avec la même cible sont requises (l'une pour le lecteur, l'autre pour le robot), mais avec des LUN différents.

Par exemple :

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

```
name="st" class="scsi"
target=1 lun=1
```

sst.conf : Périphériques de bibliothèque

Ce fichier est requis sur chaque client Solaris Data Protector auquel un périphérique de bibliothèque multi-lecteurs est connecté. D'une manière générale, il requiert une entrée pour l'adresse SCSI du mécanisme de robot de chacun des périphériques de bibliothèque connectés au client. Il existe cependant quelques exceptions, à l'instar du HP StorageWorks 24x6 mentionné dans la section précédente.

1. Copiez le pilote (module) `sst` et le fichier de configuration `sst.conf` dans le répertoire requis :
   - Pour les systèmes d'exploitation 32 bits :

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

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

   - Pour les systèmes d'exploitation 64 bits :

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

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

2. Modifiez le fichier `sst.conf` et ajoutez l'entrée suivante :

   ```
   name="sst" class="scsi" target=X lun=Y;
   ```

   où :

   X correspond à l'adresse SCSI du mécanisme du robot.

   Y est l'unité logique.

   Par exemple :

   ```
   name="sst" class="scsi" target=6 lun=0;
   ```

3. Ajoutez le pilote au noyau Solaris :

   ```
   add_drv sst
   ```

Création et vérification de fichiers de périphérique

Après avoir défini les fichiers de configuration et installé les pilotes, vous pouvez créer de nouveaux fichiers de périphérique comme suit :

1. Supprimez tous les fichiers de périphérique existants du répertoire `/dev/rmt` :

   ```
   cd /dev/rmt
   rm *
   ```

2. Tapez la commande suivante pour arrêter le système :

   ```
   shutdown -i0 -g0
   ```

3. Relancez le système :

   ```
   boot -rv
   ```

   Le commutateur `r` de la commande `boot` permet une compilation du noyau et inclut la création de fichiers de périphérique spéciaux utilisés pour la communication avec le périphérique à bandes. Le commutateur `v` active l'affichage en mode prolixe (verbose) du démarrage du système. Avec le mode prolixe, le système indique que le périphérique est connecté en affichant la chaîne *<nom de référence du périphérique à bandes>* que vous avez sélectionnée lors de la phase de l'initialisation relative à la configuration du répertoire `/devices`.

4. Tapez la commande suivante pour vérifier l'installation :

   ```
   mt -t /dev/rmt/0 status
   ```

   La sortie de cette commande dépend du lecteur configuré. Elle se présente de la manière suivante :

   ```
   Quantum DLT7000 tape drive:
   sense key(0x6)= Unit Attention   residual= 0    retries= 0
   file no= 0   block no= 0
   ```

5. Une fois que la réinitialisation est terminée, vous pouvez vérifier les fichiers de périphérique qui ont été créés à l'aide de la commande `ls -all`. Pour un périphérique de bibliothèque, le résultat de cette commande peut être le suivant :

   `/dev/rmt/0hb` pour un premier lecteur de bandes

   `/dev/rmt/1hb` pour un deuxième lecteur de bandes

   `/dev/rsst6` pour un lecteur de robot

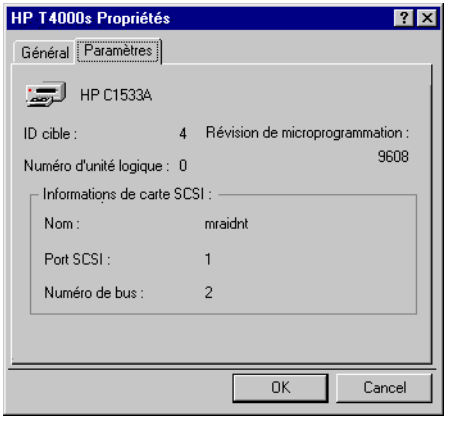
Recherche des ID SCSI cibles inutilisés sur un système Windows

Pour déterminer quels sont les ID SCSI cibles (adresses SCSI) inutilisés sur un système Windows, procédez comme suit :

1. Dans le `Panneau de configuration` Windows, cliquez deux fois sur `Adaptateurs SCSI`.
2. Vérifiez les propriétés de chaque périphérique connecté à une carte SCSI de la liste. Cliquez deux fois sur le nom d'un périphérique, puis sélectionnez `Paramètres` pour ouvrir sa page de propriétés. Voir la figure B-15 à la page B-59.

   Notez les `ID SCSI cibles` et les `LUN (Numéros d'unité logique)` affectés au périphérique. Vous pouvez ainsi savoir quels sont les `ID SCSI cibles` et `LUN` déjà occupés.

Figure B-15 Paramètres du périphérique



Configuration des ID SCSI sur une bibliothèque HP StorageWorks 330fx

Une fois que vous avez choisi les ID SCSI pour le robot et les lecteurs, vous pouvez les vérifier et les configurer à l'aide du panneau de configuration de la bibliothèque.

EXEMPLE : si vous disposez d'une bibliothèque HP StorageWorks 330fx, procédez comme suit pour trouver les ID SCSI configurés :

1. Depuis l'état PRET, appuyez sur SUIVANT. ADMIN* apparaît.
2. Appuyez sur ENTREE. Vous êtes invité à saisir le mot de passe. Saisissez le mot de passe.
3. TEST* apparaît ; appuyez sur SUIVANT jusqu'à ce que l'option ID SCSI* apparaisse.
4. Appuyez sur ENTREE. VIEW IDs* apparaît.
5. Appuyez sur ENTREE. JKBX ID 6 LUN 0 s'affiche.
6. Appuyez sur SUIVANT. DRV 1 ID 5 LUN 0 s'affiche.
7. Appuyez sur SUIVANT. DRV 2 ID 4 LUN 0 s'affiche, etc.

Vous pouvez revenir à l'état PRET en appuyant sur ANNULER plusieurs fois.

Connexion de périphériques de sauvegarde

Pour connecter un périphérique de sauvegarde à un système HP-UX, Solaris ou Windows, suivez la procédure générale ci-dessous.

1. Sélectionnez le client auquel vous souhaitez connecter le périphérique de sauvegarde.
2. Installez un Agent de support sur le système sélectionné. Reportez-vous à la section “Installation distante de clients Data Protector” à la page 54.
3. Déterminez l'adresse SCSI non occupée pouvant être utilisée par le périphérique. Pour les systèmes HP-UX, reportez-vous à la section “Recherche des adresses SCSI non utilisées sous HP-UX” à la page B-50. Pour les systèmes Solaris, reportez-vous à la section “Recherche des ID SCSI cibles inutilisés sous Solaris” à la page B-52. Pour les systèmes Windows, reportez-vous à la section “Recherche des ID SCSI cibles inutilisés sur un système Windows” à la page B-59.

   ✓ Pour la connexion à un système HP-UX, vérifiez que les pilotes requis sont *installés* et *intégrés* au noyau en cours. Pour cela, reportez-vous à la section “Vérification de la configuration du noyau sous HP-UX” à la page 75.

   Si vous devez configurer un pilote de passage SCSI, reportez-vous à la section “Configuration de robot SCSI sous HP-UX” à la page B-41.

   ✓ Pour la connexion à un système Solaris, vérifiez que les pilotes requis sont installés et que les fichiers de configuration sont à jour pour l'installation du périphérique. Reportez-vous à la section “Mise à jour de la configuration des périphériques et pilotes sur un système Solaris” à la page B-53. Celle-ci vous indique également comment mettre à jour le fichier `sst.conf` si vous devez configurer un pilote de passage SCSI.

   ✓ Si le périphérique est connecté à un client Windows, le lecteur de bande d'origine peut être chargé ou désactivé, selon la version du système Windows. Reportez-vous à la section “Utilisation de pilotes de bandes et de pilotes de robots sous Windows” à la page B-34.

Si vous chargez le pilote de bandes natif pour un périphérique déjà configuré dans Data Protector qui n'utilisait pas le pilote de bandes natif, n'oubliez pas de renommer les fichiers de périphérique pour tous les périphériques logiques Data Protector configurés qui se rapportent au périphérique en question (par exemple, remplacez `scsi1:0:4:0` par `tape3:0:4:0`).

Pour plus d'informations concernant l'attribution d'un nom de fichier de périphérique correct, reportez-vous à la section “Création de fichiers de périphérique (adresses SCSI) sous Windows” à la page B-38.

4. Définissez les adresses SCSI (ID) sur le périphérique. En fonction du type de périphérique, vous pouvez généralement effectuer cette opération avec les commutateurs du périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

   Si vous souhaitez voir un exemple, reportez-vous à la section “Configuration des ID SCSI sur une bibliothèque HP StorageWorks 330fx” à la page B-60.

   Pour obtenir des informations détaillées sur les périphériques pris en charge, reportez-vous à la page http://www.hp.com/support/manuals.

REMARQUE

Sur un système Windows NT doté d'une carte SCSI Adaptec et auquel est connecté un périphérique SCSI, vous devez activer l'option `Carte hôte BIOS` afin que le système n'ait pas de problème pour émettre les commandes SCSI.

Pour définir l'option `Carte hôte BIOS`, appuyez sur `Ctrl+A` pendant l'initialisation du système pour accéder au menu Carte SCSI, puis sélectionnez `Configurer/Afficher les paramètres de la carte hôte` -> `Options de configuration avancées`, et enfin activez `Carte hôte BIOS`.

5. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'initialisation soit terminé. Vérifiez que le système reconnaît bien le nouveau périphérique de sauvegarde.

   ✓ Sur un système HP-UX, servez-vous de l'utilitaire `ioscan`

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

pour afficher la liste des périphériques connectés, avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver le nouveau périphérique connecté avec les adresses SCSI correctes.

Si un fichier de périphérique n'a pas été créé automatiquement durant le processus d'initialisation, vous devez le créer manuellement. Reportez-vous à la section “Création de fichiers de périphérique sous HP-UX” à la page B-46.

- ✓ Sur un système Solaris, exécutez l'utilitaire `ls -all` dans le répertoire `/dev/rmt` pour afficher la liste des périphériques connectés, avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver le nouveau périphérique connecté avec les adresses SCSI correctes.
- ✓ Sur un système Windows, vous pouvez vérifier que le système reconnaît correctement le nouveau périphérique de sauvegarde à l'aide de l'utilitaire `devbra`. Dans le répertoire *<répertoire_Data_Protector>*`\bin`, exécutez :

  ```
  devbra -dev
  ```

  Dans les résultats de la commande `devbra`, vous trouverez pour chaque périphérique connecté et correctement reconnu les lignes suivantes :

  <spécification du périphérique de sauvegarde>

  <chemin_matériel>

  <type_support>

  ```
  ...........
  ```

  Par exemple, les résultats suivants :

  ```
  HP:C1533A

  tape3:0:4:0

  DDS

  ...

  ...
  ```

signifient qu'un périphérique à bandes HP DDS (le pilote de bandes natif étant chargé) a le numéro d'instance du lecteur 3, et est connecté au bus SCSI 0, à l'ID SCSI cible 4 et au numéro LUN 0.

Tandis que les résultats suivants :

```
HP:C1533A

scsi1:0:4:0

DDS

...

...
```

signifient qu'un périphérique à bandes HP DDS (le pilote de bandes d'origine étant déchargé) est connecté au port SCSI 1, au bus SCSI 0 et que le lecteur de bandes a l'ID SCSI cible 4 et le numéro LUN 0.

✓ Sur un système AIX, servez-vous de l'utilitaire `lsdev`

```
lsdev -C
```

pour afficher la liste des périphériques connectés et les noms de périphérique correspondants.

Compression matérielle

La plupart des périphériques de sauvegarde récents proposent une compression matérielle intégrée pouvant être activée lors de la création d'un fichier de périphérique ou d'une adresse SCSI pendant la procédure de configuration du périphérique. Reportez-vous à l'aide en ligne pour connaître la procédure détaillée.

La compression matérielle est effectuée par un périphérique qui reçoit les données originales d'un Agent de support et les écrit sur la bande sous forme compressée. Ce procédé permet d'augmenter la vitesse à laquelle un lecteur de bande reçoit les données car le volume de données écrit sur la bande est moins important.

Lorsque la compression logicielle est utilisée et la compression matérielle désactivée, les données sont compressées par l'Agent de disque et envoyées sous forme compressée à un Agent de support. L'algorithme de compression peut faire appel à une quantité de ressources de l'Agent de disque considérable si la compression logicielle est utilisée, mais cela réduit la charge réseau.

Pour activer la compression matérielle sous Windows, ajoutez “C” à la fin des adresses SCSI de périphérique/lecteur, par exemple : scsi:0:3:0C (ou tape2:0:1:0C si le pilote du lecteur de bandes est chargé). Si le périphérique prend en charge la compression matérielle, celle-ci sera utilisée ; sinon, l'option C sera ignorée.

Pour désactiver la compression matérielle sous Windows, ajoutez “N” à la fin des adresses SCSI de périphérique/lecteur, par exemple : scsi:0:3:0:N.

Pour activer/désactiver la compression matérielle sous UNIX, sélectionnez un fichier de périphérique approprié. Consultez la documentation du périphérique et du système d'exploitation pour plus de détails.

Etape suivante

A ce stade de la procédure, les périphériques de sauvegarde doivent être connectés afin que vous puissiez les configurer ainsi que les pools de supports. Dans l'index de l'aide en ligne, recherchez : “configuration, périphériques de sauvegarde” pour plus d'informations sur les tâches de configuration supplémentaires.

Un Agent de support doit être installé sur votre système. Pour connaître la procédure, reportez-vous à la section “Installation distante de clients Data Protector” à la page 54.

Les sections suivantes décrivent la procédure de connexion d'un périphérique à bandes autonome HP StorageWorks 24, d'une bibliothèque HP StorageWorks 12000e et d'une bibliothèque DLT 28/48 logements HP StorageWorks à des systèmes HP-UX et Windows.

Connexion d'un périphérique autonome HP StorageWorks 24

Le périphérique de sauvegarde DDS StorageWorks 24 est un lecteur de bandes autonome basé sur la technologie DDS3.

Connexion à un système HP-UX

Pour connecter un périphérique autonome HP StorageWorks 24 à un système HP-UX, procédez comme suit :

1. Vérifiez que les pilotes nécessaires (`stape` ou `tape2`) sont *installés* et *intégrés* au noyau actuel. Reportez-vous à la section “Vérification de la configuration du noyau sous HP-UX” à la page 75.
2. Définissez une adresse SCSI non occupée pouvant être utilisée par le lecteur de bandes. Reportez-vous à la section “Recherche des adresses SCSI non utilisées sous HP-UX” à la page B-50.
3. Définissez les adresses SCSI (ID) sur le périphérique. Utilisez les commutateurs situés à l'arrière du périphérique.

   Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.
4. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'initialisation soit terminé.
5. Vérifiez que le système reconnaît correctement le nouveau lecteur de bandes connecté. Servez-vous de l'utilitaire `ioscan` :

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

   pour afficher la liste des périphériques connectés avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver le nouveau lecteur de bandes connecté avec l'adresse SCSI correcte. Le fichier de périphérique du lecteur a été créé lors du processus d'amorçage.

Etape suivante

Une fois que le périphérique est correctement connecté, recherchez : “configuration, périphériques de sauvegarde” dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion à un système Windows

Pour connecter un périphérique autonome HP StorageWorks 24 à un système Windows, procédez comme suit :

1. Définissez une adresse SCSI (ID cible) non occupée pouvant être utilisée par le lecteur de bandes. Reportez-vous à la section “Recherche des ID SCSI cibles inutilisés sur un système Windows” à la page B-59.
2. Définissez les adresses SCSI (ID) sur le périphérique. Utilisez les commutateurs situés à l'arrière du périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.
3. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'initialisation soit terminé.
4. Vérifiez que le système reconnaît correctement le nouveau lecteur de bandes connecté. Exécutez la commande `devbra` à partir du répertoire `<répertoire_Data_Protector>\bin`. Tapez

   ```
   devbra -dev
   ```

   Dans les résultats de la commande `devbra`, vous devez trouver le nouveau lecteur de bandes connecté du périphérique autonome HP StorageWorks 24.

Etape suivante

Une fois que le périphérique est correctement connecté, recherchez : “configuration, périphériques de sauvegarde” dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion d'un chargeur automatique DAT HP StorageWorks

Les bibliothèques HP StorageWorks 12000e et StorageWorks DAT 24x6 sont toutes deux dotées d'un logement pour six cartouches, d'un lecteur et d'un bras robotisé utilisé pour déplacer les cartouches du/vers le lecteur. Les deux bibliothèques sont également équipées d'un système de détection de bande encrassée.

Connexion à un système HP-UX

Pour connecter le périphérique de bibliothèque HP StorageWorks 12000e à un système HP-UX, procédez comme suit :

1. A l'arrière du chargeur automatique, mettez le commutateur de mode sur `6`.
2. Vérifiez que les pilotes nécessaires (`stape` ou `tape2`) sont *installés* et *intégrés* au noyau actuel. Reportez-vous à la section “Vérification de la configuration du noyau sous HP-UX” à la page 75.
3. Vérifiez que les pilotes de passage SCSI (`sctl` ou `spt`) sont *installés* et *intégrés* au noyau actuel. Reportez-vous à la section “Configuration de robot SCSI sous HP-UX” à la page B-41.
4. Déterminez une adresse SCSI non occupée pouvant être utilisée par le lecteur de bandes et le robot. Reportez-vous à la section “Recherche des adresses SCSI non utilisées sous HP-UX” à la page B-50.

REMARQUE

La bibliothèque HP StorageWorks 12000e utilise la même adresse SCSI pour le lecteur de bandes et le robot, mais avec différents numéros LUN.

5. Définissez les adresses SCSI (ID) sur le périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.
6. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'initialisation soit terminé.
7. Vérifiez que le système reconnaît correctement le nouveau lecteur de bandes connecté. Servez-vous de l'utilitaire `ioscan`

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

   pour afficher la liste des périphériques connectés avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver le nouveau lecteur de bandes connecté avec l'adresse SCSI correcte.
8. Le fichier de périphérique du lecteur a été créé lors du processus d'amorçage, mais vous devez créer celui du robot manuellement. Reportez-vous à la section “Création de fichiers de périphérique sous HP-UX” à la page 46.

9. Vérifiez que le système reconnaît correctement le nouveau fichier de périphérique du robot de bibliothèque. Servez-vous de l'utilitaire `ioscan` :

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

   Le nouveau fichier de périphérique doit apparaître dans les résultats de la commande.

Etape suivante

Une fois que le périphérique de bibliothèque est correctement connecté, recherchez : “configuration, périphériques de sauvegarde” dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion à un système Windows

Pour connecter le périphérique de bibliothèque HP StorageWorks 12000e à un système Windows, procédez comme suit :

1. A l'arrière du chargeur automatique, mettez le commutateur de mode sur `6`.
2. Déterminez une adresse SCSI non occupée pouvant être utilisée par le lecteur de bandes et le robot. Reportez-vous à la section “Recherche des ID SCSI cibles inutilisés sur un système Windows” à la page B-59.
3. Définissez les adresses SCSI (ID) sur le périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

REMARQUE

La bibliothèque HP StorageWorks 12000e utilise la même adresse SCSI pour le lecteur de bandes et le robot, mais avec différents numéros LUN.

4. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'initialisation soit terminé.
5. Vérifiez que le système reconnaît correctement le nouveau lecteur de bandes connecté et le robot. Dans le répertoire *<répertoire_Data_Protector>*`\bin`, exécutez :

   ```
   devbra -dev
   ```

Dans les résultats de la commande `devbra`, vous devez trouver le nouveau lecteur de bandes connecté et le robot du périphérique de bibliothèque HP StorageWorks 12000e.

Etape suivante

Une fois que le périphérique de bibliothèque est correctement connecté, recherchez : “configuration, périphériques de sauvegarde” dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion d'une bibliothèque DLT 28/48 logements HP StorageWorks

La bibliothèque DLT 28/48 logements HP StorageWorks est une bibliothèque multi-lecteurs destinée aux environnements d'entreprise ayant de 80 à 600 Go à sauvegarder. Elle est équipée de quatre lecteurs DLT 4000 ou DLT 7000 dotés de plusieurs canaux de données, d'un logement de bande et d'un lecteur de codes-barres.

Connexion à un système HP-UX

Pour connecter la bibliothèque DLT 28/48 logements HP StorageWorks à un système HP-UX, procédez comme suit :

1. Vérifiez que les pilotes nécessaires (`stape` ou `tape2`) sont *installés* et *intégrés* au noyau en cours. Reportez-vous à la section “Vérification de la configuration du noyau sous HP-UX” à la page 75.
2. Vérifiez que les pilotes de passage SCSI (`sctl` ou `spt`) sont *installés* et *intégrés* au noyau actuel. Reportez-vous à la section “Configuration de robot SCSI sous HP-UX” à la page B-41.
3. Déterminez une adresse SCSI non occupée pouvant être utilisée par le lecteur de bandes et le robot. Reportez-vous à la section “Recherche des adresses SCSI non utilisées sous HP-UX” à la page B-50.

REMARQUE

La bibliothèque DLT 28/48 logements HP StorageWorks est dotée de quatre lecteurs de bande et d'un robot, vous devez donc disposer de cinq adresses SCSI inutilisées au cas où tous les lecteurs de bandes devraient être utilisés. Les lecteurs de bandes et le robot doivent utiliser des adresses SCSI différentes.

4. Définissez les adresses SCSI (ID) sur le périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.
5. Allumez le périphérique, puis l'ordinateur, et attendez que le processus d'amorçage soit terminé.
6. Vérifiez que le système reconnaît correctement les nouveaux lecteurs de bandes connectés. Servez-vous de l'utilitaire `ioscan`

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

   pour afficher la liste des périphériques connectés avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver les nouveaux lecteurs de bandes connectés avec les adresses SCSI correctes.
7. Les fichiers de périphérique des lecteurs ont été créés lors du processus d'initialisation, mais vous devez créer celui du robot manuellement. Reportez-vous à la section “Création de fichiers de périphérique sous HP-UX” à la page B-46.
8. Vérifiez que le système reconnaît correctement le nouveau fichier de périphérique du robot de bibliothèque. Servez-vous de l'utilitaire `ioscan` :

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

   Le nouveau fichier de périphérique doit apparaître dans les résultats de la commande.

Etape suivante

Une fois le périphérique de la bibliothèque DLT 28/48 logements HP StorageWorks correctement connecté, recherchez : “configuration, périphériques de sauvegarde” dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion à un système Solaris

Pour configurer le périphérique de bibliothèque HP C5173-7000 sur un système Solaris, exécutez la procédure décrite ci-dessous. Cet exemple suppose que deux lecteurs sont alloués à Data Protector :

1. Copiez le pilote (module) `sst` et le fichier de configuration `sst.conf` dans le répertoire requis :
   - Pour les systèmes d'exploitation 32 bits :

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

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

- Pour les systèmes d'exploitation 64 bits :

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

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

2. Ajoutez le pilote au noyau Solaris :

   ```
   add_drv sst
   ```

3. Supprimez tous les fichiers de périphérique existants du répertoire `/dev/rmt` :

   ```
   cd /dev/rmt
   rm *
   ```

4. Arrêtez le système en appuyant sur `Stop` et `A`.

5. Exécutez la commande `probe-scsi-all` à l'invite "`ok`" pour vérifier quelles sont les adresses SCSI disponibles.

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

   Le système peut vous demander de lancer la commande `reset-all` avant d'exécuter la commande `probe-scsi-all`.

   Dans le cas présent, nous utiliserons le port 6 pour le périphérique de contrôle SCSI, le port 2 pour le premier lecteur et le port 1 pour le deuxième lecteur ; le numéro LUN est 0.

6. Revenez en fonctionnement normal :

   ```
   ok go
   ```

7. Copiez le fichier de configuration `st.conf` dans le répertoire requis :

   ```
   $cp /opt/omni/spt/st.conf /kernel/drv/st.conf
   ```

   Le fichier `st.conf` est présent sur chaque client Data Protector Solaris et contient les adresses SCSI de chaque périphérique de sauvegarde connecté au client.

8. Modifiez le fichier `/kernel/drv/st.conf` et ajoutez les lignes suivantes :

   ```
   tape-config-list= "QUANTUM DLT7000", "Digital DLT7000",
   "DLT-data3";
   ```

```
DLT-data3 = 1,0x77,0,0x8639,4,0x82,0x83,0x84,0x85,3;

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

name="st" class="scsi"
target=2 lun=0;

name="st" class="scsi"
target=6 lun=0;
```

Ces entrées fournissent les adresses SCSI pour le lecteur 1, le lecteur 2 et le robot.

9. Modifiez le fichier `sst.conf` (que vous avez copié à l'étape 1) et ajoutez la ligne suivante :

   ```
   name="sst" class="scsi" target=6 lun=0;
   ```

   Notez que cette entrée doit être identique à celle du robot dans le fichier `st.conf`. Reportez-vous à l'étape 8 ci-dessus.

10. Arrêtez le système client et connectez le périphérique de bibliothèque.
11. Remettez le périphérique de bibliothèque sous tension, puis le système client.

    Le système s'initialise alors et crée automatiquement les fichiers de périphérique pour le robot et les lecteurs de bandes. Vous pouvez répertorier ceux-ci à l'aide de la commande `ls -all`. Dans le cas présent :

/dev/rmt/0hb	pour un premier lecteur de bandes
/dev/rmt/1hb	pour un deuxième lecteur de bandes
/dev/rsst6	pour un lecteur de robot

Etape suivante

Une fois le périphérique de la bibliothèque DLT 28/48 logements HP StorageWorks correctement connecté, recherchez : “configuration, périphériques de sauvegarde” dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion à un système Windows

Pour connecter le périphérique de bibliothèque DLT 28/48 logements HP StorageWorks à un système Windows, procédez comme suit :

1. Déterminez les adresses SCSI (ID cibles) non occupées pouvant être utilisées par le lecteur de bandes et le robot. Reportez-vous à la section “Recherche des ID SCSI cibles inutilisés sur un système Windows” à la page 59.
2. Définissez les adresses SCSI (ID cibles) sur le périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

REMARQUE

La bibliothèque DLT 28/48 logements HP StorageWorks est dotée de quatre lecteurs de bande et d'un robot, vous devez donc disposer de cinq adresses SCSI inutilisées au cas où tous les lecteurs de bandes devraient être utilisés. Les lecteurs de bande et le robot doivent utiliser des ID SCSI cibles différents.

3. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'amorçage soit terminé.
4. Vérifiez que le système reconnaît correctement les nouveaux lecteurs de bandes connectés et le robot. Dans le répertoire `<répertoire_Data_Protector>\bin`, exécutez :

   ```
   devbra -dev
   ```

   Dans le résultat de la commande `devbra`, vous devez trouver les nouveaux lecteurs de bandes connectés et le robot du périphérique de bibliothèque DLT 28/48 logements HP StorageWorks.

Etape suivante

Une fois le périphérique de la bibliothèque DLT 28/48 logements HP StorageWorks correctement connecté, recherchez : “configuration, périphériques de sauvegarde” dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion d'un lecteur de bandes Seagate Viper 200 LTO Ultrium

Le lecteur de bandes Seagate Viper 200 LTO Ultrium est un périphérique autonome pour les environnements d'entreprise avec 100 à 200 Go à sauvegarder.

Connexion à un système Solaris

Pour configurer le lecteur de bandes Seagate Viper 200 LTO Ultrium sur un système Solaris, procédez comme suit :

1. Déterminez les adresses SCSI non occupées pouvant être utilisées par le lecteur de bandes. Exécutez la commande `modinfo` ou `dmesg` pour rechercher les contrôleurs SCSI en cours d'utilisation et les périphériques SCSI cibles installés :

   ```
   dmesg | egrep "target" | sort | uniq
   ```

   Le résultat suivant doit être obtenu :

   ```
   sd32 at ithps0: target 2 lun 0
   sd34 at ithps0: target 4 lun 0
   st21 at ithps1: target 0 lun 0
   st22 at ithps1: target 1 lun 0
   ```

REMARQUE Il est recommandé d'utiliser le contrôleur SCSI `glm` ou `isp` lorsque vous connectez un périphérique Viper 200 LTO à un système Solaris. De même, il est préférable d'utiliser les contrôleurs Ultra2 SCSI ou Ultra3 SCSI.

2. Modifiez le fichier `/kernel/drv/st.conf` et ajoutez les lignes suivantes :

   ```
   tape-config-list =
   "SEAGATE ULTRIUM06242-XXX" , "SEAGATE LTO" , \
   "SEAGATE_LTO";
   SEAGATE_LTO = 1, 0x7a, 0, 0x1d679, 4, 0x00, 0x00, 0x00, \
   0x00, 1;
   ```

3. Arrêtez le système client et connectez le périphérique.
4. Remettez le périphérique sous tension, puis le système client.

Le système s'initialise alors et crée automatiquement les fichiers de périphérique pour le lecteur de bandes. Vous pouvez répertorier ceux-ci à l'aide de la commande `ls -all`.

Etape suivante

Une fois le lecteur de bandes Seagate Viper 200 LTO Ultrium correctement connecté, recherchez : “configuration, périphériques de sauvegarde” dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion à un système Windows

Pour connecter le lecteur de bandes Seagate Viper200 LTO Ultrium à un système Windows, procédez comme suit :

1. Déterminez les adresses SCSI (ID cibles) non occupées pouvant être utilisées par le lecteur de bandes. Reportez-vous à la section “Recherche des ID SCSI cibles inutilisés sur un système Windows” à la page 59.
2. Définissez les adresses SCSI (ID cibles) sur le périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.
3. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'amorçage soit terminé.
4. Vérifiez que le système reconnaît correctement les nouveaux lecteurs de bandes connectés et le robot. Dans le répertoire *<répertoire_Data_Protector>*\bin, exécutez :

   ```
   devbra -dev
   ```

   Dans les résultats de la commande `devbra`, vous devez trouver le nouveau lecteur de bandes connecté du lecteur de bandes Seagate Viper 200 LTO Ultrium.

Etape suivante

Une fois le lecteur de bandes Seagate Viper 200 LTO Ultrium correctement connecté, recherchez : “configuration, périphériques de sauvegarde” dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

REMARQUE

Lorsque vous configurez le lecteur de bandes Seagate Viper 200 LTO Ultrium avec Data Protector, assurez-vous que le mode de compression est activé. Pour cela, spécifiez le paramètre `C` après l'adresse SCSI du lecteur, par exemple :

```
scsi2:0:0:0C
```

Vérification de l'installation de l'Agent général de supports sous Novell NetWare

Après avoir effectué l'installation de l'Agent général de supports sur la plateforme Novell NetWare, vous devez la contrôler en procédant comme suit :

- ✓ Identifiez le périphérique de stockage.
- ✓ Testez le démarrage de l'Agent général de supports sur la console du serveur Novell NetWare.
- ✓ Testez le démarrage de `HPUMA.NLM` et de `HPDEVBRA.NLM` sur la console du serveur Novell NetWare.

Identification du périphérique de stockage

Utilisez la convention suivante pour identifier un périphérique de stockage dans l'environnement Novell NetWare :

<numéro d'identification de la carte>: *<numéro d'identification cible>*: *<numéro d'unité logique><compression>*

Par exemple, la chaîne "`0:2:0N`" identifie un périphérique de stockage avec comme ID de carte 0, comme ID cible 2, un numéro d'unité logique (LUN) 0 et aucune compression.

Autre exemple : la chaîne "`1:1:0C`" identifie un périphérique de stockage avec comme ID de carte 1, comme ID cible 1, un numéro d'unité logique (LUN) 0 et la compression activée.

Test de démarrage de l'Agent général de supports

Une fois l'Agent général de supports installé sur le système Novell NetWare, vous pouvez tester le démarrage d'un Agent de support de sauvegarde `HPBMA.NLM` sur la console du serveur Novell NetWare.

Dans l'exemple ci-après, la carte bus hôte `Adaptec`, `AHA-2940`, est utilisée pour accéder au périphérique à bandes échangeur de la bibliothèque de bandes HP StorageWorks 12000e.

Avant de démarrer tout composant `*.NLM` de Data Protector, vous devez satisfaire aux conditions suivantes :

- ✓ `HPINET` doit être en cours d'exécution.
- ✓ Le pilote de carte hôte SCSI `Adaptec` doit être en cours d'exécution.
- ✓ Le logiciel de l'Agent général de supports doit se trouver dans le répertoire `SYS:USR\OMNI\BIN`.
- ✓ Le périphérique de stockage doit être correctement installé et connecté.
- ✓ La carte bus hôte Adaptec et le protocole de communication TCP/IP doivent être correctement installés et en cours d'exécution.

Une fois ces conditions remplies, procédez comme suit :

1. Pour charger `HPBMA.NLM`, tapez :

   `LOAD HPBMA -name testbma -type <numéro_type> -policy <numéro_mode> -ioctl <périphérique_contrôle> -dev <périphérique_données> -tty <numéro_port_TCP>`

   L'option `type <numéro_type>` correspond au type de périphérique Data Protector. Les valeurs possibles pour `<numéro_type>` sont les suivantes :

   - 1=DAT/DDS
   - 2 = QIC (cartouche d'un quart de pouce)
   - 3 = Exabyte 8mm
   - 9 = périphérique générique à bandes magnétiques
   - 10 = bande linéaire numérique (DLT)

   L'option `policy <numéro_mode>` correspond au mode d'utilisation du périphérique par Data Protector. Les valeurs possibles sont les suivantes :

   - 1= périphérique autonome
   - 10= bibliothèque SCSI - II

   L'option `ioctl <périphérique_contrôle>` définit l'adresse SCSI du contrôle du robot. Elle se présente sous la forme suivante :

   `<numéro_identification_adaptateur>:<numéro_identification_cible>:<numéro_unité_logique>`

Par exemple :

- `0:1:1` => Le périphérique de contrôle (robot) utilise la carte SCSI 0, possède l'adresse SCSI 1 et le LUN 1.

L'option `dev` *<périphérique_données>* définit l'adresse SCSI du contrôle du robot. Elle se présente sous la forme suivante :

<numéro_identification_adaptateur>:*<numéro_identification_cible>*:*<numéro_unité_logique>*<*compression*>

Par exemple :

- `0:1:1C` => Le périphérique de contrôle (robot) utilise la carte SCSI 0, possède l'adresse SCSI 1 et le LUN 1. La compression de données est activée.

L'option `-tty` *<numéro_port_TCP>* correspond au numéro de port du protocole de communication TCP/IP.

L'Agent de support de la console, `HPCONMA.NLM`, démarre et l'écran suivant s'affiche :

```
*** MA listening on port: <numéro>
```

SLOT: [Load(2), Peek(2), Stop(0), Abort(0)]

```
SLOT: _
```

Les commandes actuellement disponibles sont les suivantes :

`Load(2)` - Cette commande permet de charger la bande dans le lecteur et requiert deux arguments :

`Load` *<numéro d'emplacement> <indicateur de permutation>*

L'indicateur de permutation peut être défini soit à 0 soit à 1, ce qui signifie que le support ne permute pas si la valeur est 0 ou qu'il permute si la valeur est 1.

`Stop(0)` - Termine normalement la session en cours.

`Abort(0)` - Abandonne la session en cours.

Dans cet exemple, vous chargez la bande à partir de l'emplacement 3 (`SLOT 3`) sans permutation du support.

2. Tapez la commande permettant de charger la bande à partir de l'emplacement 3 (`SLOT 3`) sans permutation du support.

```
SLOT:LOAD 3 0
```

Une fois la bande chargée dans le lecteur, le message suivant s'affiche :

```
CHECK: [Deny(0), Init(1), Seek(2), Abort(0)]
CHECK: _
```

Les commandes disponibles sont les suivantes :

`Deny(0)` - Refuse l'action en cours.

`Init(1)` - Initialise la bande chargée et requiert un paramètre :

`Init(1)` *<ID du support>*

`Seek(2)` - Effectue une recherche à la position requise. La chaîne d'arguments est la suivante :

`Seek`*<numéro de segment> <numéro de bloc>*

`Abort(0)` - Abandonne la session en cours.

3. Pour initialiser la bande, tapez

   ```
   CHECK: Init test
   ```

4. Basculez de l'écran de l'Agent général de supports de sauvegarde à la console Novell NetWare et démarrez la session de sauvegarde à l'aide de la commande d'action/de requête de l'Agent de support.

REMARQUE Vous devez démarrer l'Agent de disque Data Protector sur l'hôte sélectionné en entrant `load -ma` *<hôte> <port>* pour permettre une communication correcte entre l'Agent général de supports et l'Agent de disque et afficher le bon numéro de port des opérations de la session de sauvegarde lorsque `HPCONMA.NLM` démarre. Une fois la session de sauvegarde terminée correctement, un message s'affiche.

5. Pour quitter correctement l'Agent de support de sauvegarde, appuyez sur `<CTRL-C>` lorsque l'écran de l'`Agent de support de sauvegarde` s'affiche. L'invite `Requête d'intervention sur la console` s'affiche au bout de quelques secondes :

   ```
   ATT:[Stop(0), Abort(0), Disconnect(1)]
   ```
   Exécutez la commande `Stop` pour terminer la session.

Test du démarrage de HPUMA.NLM et de HPDEVBRA.NLM

Le chargement de `HPUMA.NLM` sur la console du serveur permet de tester manuellement les commandes SCSI.

Chargez `HPUMA.NLM` à l'aide de la commande suivante :

`LOAD HPUMA.NLM -ioctl <périphérique_contrôle> -dev <périphérique_données> -tty`

L'option `ioctl <périphérique_contrôle>` définit l'adresse SCSI du contrôle du robot. Elle se présente sous la forme suivante :

<numéro_identification_adaptateur>:*<numéro_identification_cible>*:*<numéro_unité_logique>*

Par exemple :

- `0:1:1` => Le périphérique de contrôle (robot) utilise la carte SCSI 0, possède l'adresse SCSI 1 et utilise le LUN 1.

L'option `dev <périphérique_données>` définit l'adresse SCSI du contrôle du robot. Elle se présente sous la forme :

<numéro_identification_adaptateur>:*<numéro_identification_cible>*:*<numéro_unité_logique>*:*<compression>*

Par exemple :

- `0:1:1C` => Le périphérique de contrôle (robot) utilise la carte SCSI 0, possède l'adresse SCSI 1 et le LUN 1. La compression de données est activée.

L'option `-tty` est nécessaire pour interagir avec la console du serveur Novell NetWare.

HPUMA démarre et l'écran suivant s'affiche :

`prompt>`

où "prompt" se présente sous la forme suivante :
`<numéro_identification_adaptateur>:<numéro_identification_cible>:<numéro_unité_logique>`
Par exemple :

`0:2:1>`

Pour afficher les commandes actuellement disponibles, tapez la commande `HELP` dans l'écran HPUMA. Par exemple, tapez `STAT` à l'invite pour voir si les logements et le ou les lecteurs sont occupés ou vides.

Lorsque vous avez terminé, tapez `BYE` pour fermer l'écran HPUMA.

Le chargement de `HPDEVBRA.NLM` vous permet localement d'obtenir des informations sur les périphériques à la fois installés et détectés sur le serveur Novell NetWare.

Pour charger `HPDEVBRA.NLM` sur la console du serveur, entrez la commande suivante :

```
LOAD HPDEVBRA.NLM -dev
```

où l'option `-dev` est nécessaire pour répertorier tous les périphériques associés au serveur Novell NetWare.

Pour afficher les commandes disponibles, chargez `HPDEVBRA.NLM` avec l'option `HELP` :

```
LOAD HPDEVBRA -HELP
```

Installation de Data Protector sur Microsoft Cluster avec Veritas Volume Manager

Pour installer Data Protector sur Microsoft Cluster Server (MSCS) avec Veritas Volume Manager, commencez par suivre la procédure d'installation de Data Protector sur MSCS. Reportez-vous à la section “Installation de Data Protector sur Microsoft Cluster Server” à la page 179.

Une fois que vous avez terminé l'installation, certaines étapes supplémentaires sont requises pour activer le service `Data Protector Inet` permettant de distinguer, entre les ressources disque de cluster et les ressources disque locales, celles qui utilisent leurs propres ressources et non le pilote de ressources Microsoft :

1. Exécutez la commande `omnisv -stop` sur le Gestionnaire de cellule pour arrêter les services et processus Data Protector :

   `<répertoire_Data_Protector>\bin\omnisv -stop`

2. Définissez une nouvelle variable d'environnement système `OB2CLUSTERDISKTYPES` avec `Volume Manager Disk Group` en tant que valeur, ou définissez la variable `omnirc` sur les deux nœuds de cluster comme suit :

   ```
   OB2CLUSTERDISKTYPES=Volume Manager Disk Group
   ```

   Si vous souhaitez spécifier des ressources disque propriétaires supplémentaires, telles qu'un disque NetRAID4, ajoutez simplement le nom du type de la ressource à la valeur de la variable d'environnement `OB2CLUSTERDISKTYPES` :
   `OB2CLUSTERDISKTYPES=Volume Manager Disk Group;NETRaid4M Diskset`

   Pour plus d'informations sur l'utilisation des variables de fichier `omnirc`, reportez-vous au *Guide de dépannage HP OpenView Storage Data Protector*.

3. Exécutez la commande `omnisv -start` pour démarrer les services/processus :

   `<répertoire_Data_Protector>\bin\omnisv -start`

Modification du chemin des fichiers de configuration dans Data Protector A.06.00

Les chemins par défaut de certains fichiers de configuration, fichiers journaux et de base de données (sous UNIX) ont été modifiés dans Data Protector A.06.00. Certains fichiers figurant dans les répertoires `server` et `client` sont désormais divisés.

Consultez les tableaux suivants pour prendre connaissance des changements et modifiez les chemins, le cas échéant.

Fichiers de configuration sous UNIX

Fichiers de configuration client

Le tableau suivant indique les fichiers et le répertoire qui ont été déplacés du répertoire `/etc/opt/omni` vers le répertoire `/etc/opt/omni/client` pendant la mise à niveau.

Tableau B-1 Contenu du nouveau répertoire `/etc/opt/omni/client`

Ancien chemin	Chemin actuel
`/etc/opt/omni/cell/cell_server`	`/etc/opt/omni/client/cell_server`
`/etc/opt/omni/cell/omni_format`	`/etc/opt/omni/client/omni_format`
`/etc/opt/omni/cell/omni_info`	`/etc/opt/omni/client/omni_info`
`/etc/opt/omni/cell/allow_hosts`	`/etc/opt/omni/client/allow_hosts`
`/etc/opt/omni/cell/deny_hosts`	`/etc/opt/omni/client/deny_hosts`
`/etc/opt/omni/customize`	`/etc/opt/omni/client/customize`

Fichiers de configuration et fichiers journaux du Gestionnaire de cellule

Le reste du contenu du répertoire `/etc/opt/omni` a été déplacé vers le répertoire `/etc/opt/omni/server`. Par exemple, le fichier `/etc/opt/omni/cell/cell_info` se trouve désormais dans le répertoire `/etc/opt/omni/server/cell`.

Le tableau suivant indique les fichiers et le répertoire qui ont été déplacés du répertoire `/var/opt/omni` vers le répertoire `/var/opt/omni/server` pendant la mise à niveau.

Tableau B-2 Contenu du nouveau répertoire `/var/opt/omni/server`

Ancien chemin	Chemin actuel
`/var/opt/omni/db40`	`/var/opt/omni/server/db40`
`/var/opt/omni/sessions`	`/var/opt/omni/server/sessions`
`/var/opt/omni/log/<fichier_journal>`	`/var/opt/omni/server/log/<fichier_journal>`

où *<fichier_journal>* représente n'importe lequel des fichiers suivants : `HealthCheck.log`, `Check_*.txt`, `Ob2Event*`, `lic.log`, `omnisv.log`, `media.log`, `sm.log`, `crsevents.log`, `security.log`, `purge.log`, `readascii.log`, `cleaning.log`, `upgrade.log`, `trace.log` et `cluster.log`.

Tous les autres répertoires (par exemple, `/var/opt/omni/tmp`, `/var/opt/omni/windu` ou `/var/opt/omni/emc`) ainsi que les fichiers journaux (par exemple, `/var/opt/omni/log/debug.log`) n'ont pas été déplacés.

Fichiers de configuration sous Windows

Fichiers de configuration client

Le tableau suivant représente les fichiers et répertoires qui ont été déplacés du répertoire *<répertoire_Data_Protector>*`\Config` vers les répertoires *<répertoire_Data_Protector>*`\Config\client` et *<répertoire_Data_Protector>*`\tmp` pendant la mise à niveau.

Tableau B-3 Contenu du nouveau répertoire *<répertoire_Data_Protector>*`\Config\client`

Ancien chemin	Chemin actuel
<répertoire_Data_Protector>`\Config\cell\cell_server`	*<répertoire_Data_Protector>*`\Config\client\cell_server`
<répertoire_Data_Protector>`\Config\cell\omni_format`	*<répertoire_Data_Protector>*`\Config\client\omni_format`
<répertoire_Data_Protector>`\Config\cell\omni_info`	*<répertoire_Data_Protector>*`\Config\client\omni_info`

Tableau B-3 Contenu du nouveau répertoire *<répertoire_Data_Protector>*\Config\client

Ancien chemin	Chemin actuel
<répertoire_Data_Protector>\Config\cell\allow_hosts	*<répertoire_Data_Protector>*\Config\client\allow_hosts
<répertoire_Data_Protector>\Config\cell\deny_hosts	*<répertoire_Data_Protector>*\Config\client\deny_hosts
<répertoire_Data_Protector>\Config\EMC	*<répertoire_Data_Protector>*\Config\client\EMC
<répertoire_Data_Protector>\Config\tmp\EMC	*<répertoire_Data_Protector>*\tmp\EMC

Fichiers de configuration du Gestionnaire de cellule

Le reste du contenu du répertoire *<répertoire_Data_Protector>*\Config a été déplacé vers le répertoire *<répertoire_Data_Protector>*\Config\Server. Par exemple, le fichier *<répertoire_Data_Protector>*\Config\cell\cell_info se trouve désormais dans le répertoire *<répertoire_Data_Protector>*\Config\Server\cell.

Fichiers journaux

Les fichiers suivants ont été déplacés du répertoire *<répertoire_Data_Protector>*\log vers le répertoire *<répertoire_Data_Protector>*\log\server : HealthCheck.log, Check_*.txt, Ob2Event*, lic.log, omnisv.log, media.log, sm.log, crsevents.log, security.log, purge.log, readascii.log, cleaning.log, upgrade.log, trace.log et cluster.log.

Tous les autres fichiers journaux (par exemple, *<répertoire_Data_Protector>*\log\debug.log) ne sont pas déplacés.

Modifications de la ligne de commande après la mise à niveau vers Data Protector A.06.00

Les commandes répertoriées dans ce chapitre ont été modifiées ou proposent des fonctionnalités étendues concernant de nouvelles options dans Data Protector A.06.00. Vérifiez et modifiez les scripts utilisant les anciennes commandes. Sur les synopsis d'utilisation, reportez-vous aux pages man correspondantes.

Selon la version d'origine de la mise à niveau de votre Gestionnaire de cellule, reportez-vous au tableau correspondant :

- Pour la mise à niveau à partir de Data Protector A.05.00, reportez-vous au tableau B-4 à la page B-88.
- Pour la mise à niveau à partir de Data Protector A.05.10, reportez-vous au tableau B-5 à la page B-96.
- Pour la mise à niveau à partir de Data Protector A.05.50, reportez-vous au tableau B-4 à la page B-88.

Tableau B-4 Mise à niveau à partir de Data Protector A.05.00

Commande	Sous-commande/Option	Etat
ob2install	-sapdb	NOUVEAUX COMPOSANTS LOGICIELS
	-smisa	
	-db2	
	-acs	COMPOSANTS OBSOLETES DU LOGICIEL
	-das	
omniamo		NOUVELLE COMMANDE

Tableau B-4 Mise à niveau à partir de Data Protector A.05.00

Commande	Sous-commande/Option	Etat
omnib	-db2_list	NOUVELLES INTEGRATIONS
	-msvssw_list	
	-sapdb_list	
	-mbx_list	
	-share_info	NOUVELLES OPTIONS
	-miroir	
	-enh_incr	
omnicc	-check_licenses	NOUVELLES OPTIONS
	-detail	
	-update_all	
	-force_cs	
	-list_trusted_hosts	
	-secure_client	
	-unsecure_client	
	-trusted_hosts	
omnicheck		NOUVELLE COMMANDE
omniclus	-applid	OPTION MODIFIEE

Tableau B-4 Mise à niveau à partir de Data Protector A.05.00

Commande	Sous-commande/Option	Etat
omnicreatedl	-snapshot	NOUVELLES OPTIONS POUR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-smis	
	-instant_recovery	
	-snapshots *<numéro>*	
	-snapshot_type standard	
	-snapshot_type vsnap	
	-snapshot_type clone	
	-snapshot_policy strict	
	-snapshot_policy loose	
	-wait_clonecopy *<numéro>*	
	-replica_conf local	
	-replica_conf combined	
	-ca_failover_option follow_replica_direction	
	-ca_faiover_option maintain_replica_location	

Tableau B-4 Mise à niveau à partir de Data Protector A.05.00

Commande	Sous-commande/Option	Etat
omnidb	-db2	NOUVELLES INTEGRATIONS
	-vss	
	-sapdb	
	-mbx	
	-copyid	NOUVELLES OPTIONS
	-listcopies	
omnidbsmis		NOUVELLE COMMANDE
omnidbupgrade		NOUVELLE COMMANDE
omnidbutil	-extendtblspace	NOUVELLE OPTION
	-readdb	OPTION MODIFIEE
omnidbvss		NOUVELLE COMMANDE
omnidlc		NOUVELLE COMMANDE
omniinstlic		NOUVELLE COMMANDE
omniiso		NOUVELLE COMMANDE
omnimcopy	-permanent|-until	NOUVELLE OPTION

Tableau B-4 Mise à niveau à partir de Data Protector A.05.00

Commande	Sous-commande/Option	Etat
omnimm	-[no_]free_pool	OPTION MODIFIEE
	-create_free_pool	NOUVELLE OPTION
omnimigrate.pl		NOUVELLE COMMANDE
omniminit	-[no]barcode_as_label	NOUVELLE OPTION
omniobjcopy		NOUVELLE COMMANDE
omniobjconsolidate		NOUVELLE COMMANDE

Tableau B-4 Mise à niveau à partir de Data Protector A.05.00

Commande	Sous-commande/Option	Etat
omnir	-db2	NOUVELLES INTEGRATIONS
	-sapdb	
	-newinstance	NOUVELLES OPTIONS POUR SAP DB
	-recover	
	-endlogs	
	-time	
	-nochain	
	-destination	
	-from_disk	
	-instance	
	-force_prp_replica	NOUVELLE OPTION POUR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-instance *<NomInstanceSource>*	NOUVELLES OPTIONS POUR MS SQL
	-destinstance *<NomInstanceDestination>*	
	-asbase *<NomNouvelleBDD>*	
	-file *<NomFichierLogique>*	

Tableau B-4 Mise à niveau à partir de Data Protector A.05.00

Commande	Sous-commande/Option	Etat
omnir	-instance	NOUVELLES OPTIONS POUR IBM DB2 UDB
	-logfile	
	-newdbname	
	-offline	
	-rollforward	
	-tsname	
	-msvssw	NOUVELLES INTEGRATIONS
	-mbx	
	-share_info	NOUVELLE OPTION
	-oracle	NOUVELLES OPTIONS DE RESTAURATION INSTANTANEE ORACLE ET SAP R/3
	-sap	
	-user	
	-group	
	-recover	
	-restore *<arborescence>*	
	-open	
	-resetlogs	
	-paralleism	
	-restore	NOUVELLES OPTIONS DE RESTAURATION INSTANTANEE VSS
	-session	
	-vss	
	-copyid	NOUVELLE OPTION

Tableau B-4 Mise à niveau à partir de Data Protector A.05.00

Commande	Sous-commande/Option	Etat
omnirpt	media_list_extended	NOUVEAU RAPPORT
	-smtp	NOUVELLE OPTION
omniresolve		NOUVELLE COMMANDE
omnisetup.sh	-CM	NOUVELLES OPTIONS
	-IS	
	-autopass	
	db2	NOUVEAUX COMPOSANTS LOGICIELS
	smisa	
	sapdb	
	acs	COMPOSANTS OBSOLETES DU LOGICIEL
	das	
omnisrdupdate	-asr	NOUVELLES OPTIONS
	-location	
omniusers		NOUVELLE COMMANDE
sanconf	-[no_]multipath	NOUVELLES OPTIONS
	-remove_hosts	
	-sanstableaddressing	
uma	-scsiType	remplacée par l'option -interface
	-interface	remplace l'option -scsiType

Tableau B-4 Mise à niveau à partir de Data Protector A.05.00

Commande	Sous-commande/Option	Etat
upgrade_cm_from_evaa		NOUVELLE COMMANDE

Tableau B-5 Mise à niveau à partir de Data Protector A.05.10

Commande	Sous-commande/Option	Etat
ob2install	-sapdb	NOUVEAUX COMPOSANTS LOGICIELS
	-smisa	
	-acs	COMPOSANTS OBSOLETES DU LOGICIEL
	-das	
omnib	-sapdb_list	NOUVELLE INTEGRATION
	-vss_list	OPTION OBSOLETE
	-msvssw_list	NOUVELLES OPTIONS
	-share_info	
	-miroir	
	-enh_incr	

Tableau B-5 Mise à niveau à partir de Data Protector A.05.10

Commande	Sous-commande/Option	Etat
omnicc	-check_licenses	NOUVELLES OPTIONS
	-detail	
	-update_all	
	-force_cs	
	-list_trusted_hosts	
	-secure_client	
	-unsecure_client	
	-trusted_hosts	
omniclus	-applid	OPTION MODIFIEE
omnicreatedl	-smis	NOUVELLES OPTIONS POUR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-instant_recovery	
	-snapshots *<numéro>*	
	-snapshot_type clone	
	-wait_clonecopy *<numéro>*	
	-replica_conf local	
	-replica_conf combined	
	-ca_failover_option follow_replica_direction	
	-ca_faiover_option maintain_replica_location	

Tableau B-5 Mise à niveau à partir de Data Protector A.05.10

Commande	Sous-commande/Option	Etat
omnidb	-sapdb	NOUVELLE INTEGRATION
	-copyid	NOUVELLES OPTIONS
	-listcopies	
omnidbeva		COMMANDE OBSOLETE
omnidbsmis		NOUVELLE COMMANDE
omidbupgrade		NOUVELLE COMMANDE
omnidbvss		NOUVELLE COMMANDE
omnidbutil	-extendtblspace	NOUVELLE OPTION
	-readdb	OPTION MODIFIEE
omnidlc		NOUVELLE COMMANDE
omnimigrate.pl		NOUVELLE COMMANDE
omniminit	-[no]barcode_as_label	NOUVELLE OPTION
omnimm	-[no_]free_pool	OPTION MODIFIEE
	-create_free_pool	NOUVELLE OPTION
omniinstlic		NOUVELLE COMMANDE

Tableau B-5 Mise à niveau à partir de Data Protector A.05.10

Commande	Sous-commande/Option	Etat
`omniiso`		NOUVELLE COMMANDE
`omniobjcopy`		NOUVELLE COMMANDE
`omniobjconsolidate`		NOUVELLE COMMANDE

Tableau B-5 Mise à niveau à partir de Data Protector A.05.10

Commande	Sous-commande/Option	Etat
omnir	-sapdb	NOUVELLE INTEGRATION
	-newinstance	NOUVELLES OPTIONS POUR SAP DB
	-recover	
	-endlogs	
	-time	
	-nochain	
	-destination	
	-from_disk	
	-instance	
	-force_prp_replica	NOUVELLE OPTION POUR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-instance *<NomInstanceSource>*	NOUVELLES OPTIONS POUR MS SQL
	-destinstance *<NomInstanceDestination>*	
	-asbase *<NomNouvelleBDD>*	
	-file *<NomFichierLogique>*	

Tableau B-5 Mise à niveau à partir de Data Protector A.05.10

Commande	Sous-commande/Option	Etat
omnir	-oracle	NOUVELLES OPTIONS DE RESTAURATION INSTANTANEE ORACLE ET SAP R/3
	-sap	
	-user	
	-group	
	-recover	
	-open	
	-resetlogs	
	-paralleism	
	-public	NOUVELLES OPTIONS POUR MS EXCHANGE SINGLE MAILBOX
	-originalfolder	
	-keep_msg	
	-overwrite_msg	
	-folder	
	-exclude	
	-restore	NOUVELLES OPTIONS DE RESTAURATION INSTANTANEE VSS
	-session	
	-vss	
	-copyid	NOUVELLE OPTION
omnirpt	-smtp	NOUVELLE OPTION
omniresolve		NOUVELLE COMMANDE

Tableau B-5 Mise à niveau à partir de Data Protector A.05.10

Commande	Sous-commande/Option	Etat
omnisetup.sh	-CM	NOUVELLES OPTIONS
	-IS	
	-autopass	
	smisa	NOUVEAUX COMPOSANTS LOGICIELS
	sapdb	
	acs	COMPOSANTS OBSOLETES DU LOGICIEL
	das	
omniusers		NOUVELLE COMMANDE
sanconf	-[no_]multipath	NOUVELLES OPTIONS
	-remove_hosts	
	-sanstableaddressing	
upgrade_cm_from_evaa		NOUVELLE COMMANDE

Tableau B-6 Mise à niveau à partir de Data Protector A.05.50

Commande	Sous-commande/Option	Etat
omnib	-enh_incr	NOUVELLE OPTION

Tableau B-6 Mise à niveau à partir de Data Protector A.05.50

Commande	Sous-commande/Option	Etat
omnidbsmis	-ssl	NOUVELLES OPTIONS
	-caconf	
	-init	
	-put *<nom_de_fichier>*	
	-get *<nom_de_fichier>*	
	-list *<Nom EVA>*	
	-check *<Nom groupe RD>*	
omnidbeva		COMMANDE OBSOLETE
omnicreatedl	-replica_conf local	NOUVELLES OPTIONS POUR HP StorageWorks ENTERPRISE VIRTUAL ARRAY
	-replica_conf combined	
	-ca_failover_option follow_replica_direction	
	-ca_faiover_option maintain_replica_location	
omnidbutil	-extendtblspace	NOUVELLE OPTION
	-readdb	OPTION MODIFIEE
omnidbvss		NOUVELLE COMMANDE
omnidlc	-debug_loc	NOUVELLE OPTION

Tableau B-6 Mise à niveau à partir de Data Protector A.05.50

Commande	Sous-commande/Option	Etat
omnimigrate.pl		COMMANDE MISE A JOUR
omnimm	-[no_]free_pool	OPTION MODIFIEE
	-create_free_pool	NOUVELLE OPTION
omniobjconsolidate		NOUVELLE COMMANDE
omnir	-public	NOUVELLES OPTIONS POUR MS EXCHANGE SINGLE MAILBOX
	-originalfolder	
	-keep_msg	
	-overwrite_msg	
	-folder	
	-exclude	
	-restore	NOUVELLES OPTIONS DE RESTAURATION INSTANTANEE VSS
	-session	
	-vss	
omnirpt	-smtp	NOUVELLE OPTION
upgrade_cm_from_evaa		NOUVELLE COMMANDE
upgrade_cfg_from_evaa		COMMANDE OBSOLETE

C Annexe C

Utilisation de CD-ROM comme supports d'installation

Data Protector A.06.00 est également disponible sur CD-ROM. Les tâches à réaliser avant et après l'installation ainsi que les configurations système sont les mêmes que pour une installation à partir du DVD-ROM. Cependant, les procédures d'installation pour les plates-formes HP-UX, Solaris ou Linux comportent des étapes supplémentaires car vous devez utiliser plusieurs CD-ROM pour une même plate-forme.

Cette annexe décrit la structure du produit sur les CD-ROM d'installation, les différences dans les procédures d'installation et les contraintes supplémentaires inhérentes à l'installation à partir de CD-ROM.

CD-ROM d'installation Data Protector

Data Protector prend en charge différents systèmes d'exploitation sur plusieurs architectures de processeur. Par conséquent, 15 CD-ROM sont nécessaires pour couvrir toutes les plates-formes. Pour plus de détails sur le contenu des différents CD-ROM, reportez-vous à la section “Liste des CD-ROM Data Protector” à la page C-3.

Un CD-ROM spécifique pour la plate-forme HP-UX, Solaris ou Linux est mentionné dans la documentation et correspond au composant Data Protector qu'il permet d'installer, c'est-à-dire : **CD-ROM d'installation**

du Gestionnaire de cellule pour le CD-ROM utilisé pour l'installation de ce dernier et **CD-ROM d'installation du Serveur d'installation** pour le CD-ROM qui contient le Serveur d'installation et les clients.

Tableau C-1 Liste des CD-ROM Data Protector

N° de CD-ROM	Titre du CD-ROM	Sommaire
1	HP Data Protector pour HP-UX PA-RISC - Gestionnaire de cellule *Référence : CD-ROM d'installation du* Gestionnaire de cellule HP-UX de Data Protector.	• Gestionnaire de cellule pour HP-UX 11.x (architecture PA-RISC) • Tous les manuels en anglais au format PDF (dans le répertoire `DOCS`) • Packages d'intégration OpenView pour HP-UX • AutoPass pour HP-UX • Script d'installation `Omnisetup.sh`
2 3	HP Data Protector pour HP-UX PA-RISC - Serveur d'installation *Référence* : CD-ROM d'installation 1 et 2 du Serveur d'installation HP-UX de Data Protector.	• Serveur d'installation HP-UX 11.x (architecture PA-RISC) incluant tous les clients UNIX • Script d'installation `Omnisetup.sh`
4	HP Data Protector pour HP-UX IA-64 - Gestionnaire de cellule *Référence* : CD-ROM d'installation du Gestionnaire de cellule HP-UX.	• Gestionnaire de cellule pour HP-UX 11.23 (architecture IA-64) • Répertoire `DOCS` contenant tous les manuels en anglais au format PDF • Packages d'intégration OpenView pour HP-UX • AutoPass pour HP-UX • Script d'installation `Omnisetup.sh`
5 6	HP Data Protector pour HP-UX IA-64 - Serveur d'installation *Référence* : CD-ROM d'installation 1 et 2 du Serveur d'installation HP-UX de Data Protector.	• Serveur d'installation pour HP-UX 11.23.x (architecture IA-64) incluant tous les clients UNIX • Script d'installation `Omnisetup.sh`

Tableau C-1 Liste des CD-ROM Data Protector

N° de CD-ROM	Titre du CD-ROM	Sommaire
7	HP Data Protector pour Solaris - Gestionnaire de cellule *Référence* : CD-ROM d'installation du Serveur d'installation Solaris de Data Protector.	• Gestionnaire de cellule pour Solaris 8/9/10 • Tous les manuels en anglais au format PDF (dans le répertoire `DOCS`) • Packages d'intégration OpenView pour Solaris • AutoPass pour Solaris • Script d'installation `Omnisetup.sh`
8 9	HP Data Protector pour Solaris - Serveur d'installation *Référence* : CD-ROM d'installation 1 et 2 du Serveur d'installation Solaris de Data Protector.	• Serveur d'installation pour Solaris 8/9/10, y compris tous les clients UNIX[a] • Script d'installation `Omnisetup.sh`
10	HP Data Protector pour Linux x86-64 - Gestionnaire de cellule *Référence* : CD-ROM d'installation du Gestionnaire de cellule Linux de Data Protector.	• Gestionnaire de cellule pour Linux • Tous les manuels en anglais au format PDF (dans le répertoire `DOCS`) • Script d'installation `Omnisetup.sh`
11 12	HP Data Protector pour Linux x86-64 - Serveur d'installation *Référence* : CD-ROM d'installation 1 et 2 du Serveur d'installation Linux de Data Protector.	• Serveur d'installation Linux incluant tous les clients UNIX[a] • Script d'installation `Omnisetup.sh`

Tableau C-1 Liste des CD-ROM Data Protector

N° de CD-ROM	Titre du CD-ROM	Sommaire
13	Data Protector pour Windows - Gestionnaire de cellule et Serveur d'installation. Inclut des agents pour les clients Netware *Référence* : CD-ROM d'installation Windows de Data Protector.	• Gestionnaire de cellule pour Windows • Serveur d'installation pour Windows • Clients Novell NetWare • Tous les manuels en anglais au format PDF (dans le répertoire `Docs`) • AutoPass pour Windows • Produit de démonstration pour plates-formes Windows • Informations sur le produit
14	Intégrations de HP Data Protector avec OpenView, Open File Backup et les agents pour les clients OpenVMS et MPE.	• Intégrations OpenView • Package d'installation Open File Manager • Clients OpenVMS • Clients MPE • Tous les manuels en anglais au format PDF (dans le répertoire `Docs`) • Informations sur le produit
15	HP OpenView Storage Data Protector - Media Operations pour Windows	• Package d'installation pour Media Operations • Documentation pour Media Operations

a. Impossible d'installer les clients UNIX en local à partir du CD-ROM d'installation du Serveur d'installation Solaris ou Linux. Utilisez plutôt un des CD-ROM du Serveur d'installation HP-UX.

Etapes et tâches supplémentaires pour l'installation de Data Protector à partir de CD-ROM

La procédure d'installation de Data Protector à partir de CD-ROM est similaire à la procédure d'installation à partir d'un DVD-ROM.

- ***Sous UNIX***, les packages d'installation sont répartis sur *3 CD-ROM* (un pour le Gestionnaire de cellule et deux pour le Serveur d'installation) ; il est donc nécessaire de lancer les CD-ROM supplémentaires pour poursuivre l'installation.
- ***Sous Windows***, à chaque plate-forme correspond *1 CD-ROM* ; par conséquent, la procédure d'installation Windows à partir d'un CD-ROM est la même qu'à partir d'un DVD-ROM, sauf le chemin d'installation :

  Systèmes 32 bits : `\i386\setup.exe`

  Systèmes 64 bits : `\x8664\setup.exe`

Installation du Gestionnaire de cellule UNIX à partir de CD-ROM

CONSEIL

Si vous installez le Gestionnaire de cellule et le Serveur d'installation sur le même système, vous pouvez exécuter l'installation en une seule opération. Pour cela, copiez le répertoire DP_DEPOT sur le disque et exécutez la commande `omnisetup.sh -CM -IS1 -IS2`.

Pour obtenir une description de la commande `omnisetup.sh`, consultez le fichier `LISEZMOI` se trouvant dans le répertoire *<point_de_montage>*`/LOCAL_INSTALL` sur le CD-ROM ou le document *Référence de l'interface de ligne de commande HP OpenView Storage Data Protector* se trouvant dans le répertoire *<point_de_montage>*`/DOCS/C/MAN` sur le CD-ROM.

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

1. Insérez et montez le CD-ROM d'installation du Gestionnaire de cellule approprié sur un point de montage.

   Par exemple :

   ```
   mkdir /cdrom
   mount /dev/dsk/c0t0d0 /cdrom
   ```

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

- Pour copier les répertoires DP_DEPOT, LOCAL_INSTALL et AUTOPASS (où se trouvent les fichiers d'installation) sur votre disque local, exécutez la commande suivante :

  ```
  mkdir <répertoire>
  cp -r /cdrom/DP_DEPOT <répertoire>
  cp -r /cdrom/LOCAL_INSTALL <répertoire>
  cp -r /cdrom/AUTOPASS <répertoire>
  ```

- Pour copier l'ensemble du CD-ROM sur votre disque local, exécutez la commande :

  ```
  cp -r /cdrom <rép_image_cd>
  ```

2. Exécutez la commande omnisetup.sh.

   Pour lancer cette commande à partir du CD-ROM, saisissez :

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

   Pour lancer l'installation à partir du disque :

   - Si vous avez copié les répertoires DP_DEPOT, LOCAL_INSTALL et AUTOPASS à partir du CD-ROM sur votre disque local sous <répertoire>, allez sur le répertoire qui contient le fichier omnisetup.sh et exécutez la commande suivante :

     ```
     cd <répertoire>/LOCAL_INSTALL
     ./omnisetup.sh -CM
     ```

   - Si vous avez copié l'ensemble du CD-ROM dans <rép_image_cd>, exécutez la commande omnisetup.sh avec le paramètre -CM :

     ```
     cd <rép_image_cd>/LOCAL_INSTALL
     ./omnisetup.sh -CM
     ```

3. ***Sous HP-UX et Solaris,*** omnisetup.sh vous invite à installer ou à mettre à niveau l'utilitaire HP OpenView AutoPass, si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à la section “Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP OpenView AutoPass” à la page 334. L'installation d'AutoPass est recommandée.

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

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

Sous Linux, HP OpenView AutoPass n'est pas installé.

REMARQUE

Si vous avez installé le Gestionnaire de cellule sous Solaris 9, installez l'Agent de disque à distance sur le Gestionnaire de cellule à l'aide d'un Serveur d'installation. L'Agent de disque générique Solaris sera ainsi remplacé par l'Agent de disque Solaris 9. Reportez-vous à la section “Installation distante de clients Data Protector” à la page 54 ou à la page man de `ob2install`.

Installation du Serveur d’installation UNIX à partir de CD-ROM

Le Serveur d’installation UNIX est réparti sur deux CD d'installation. Par conséquent, il faut poursuivre la procédure d'installation avec le deuxième CD du Serveur d’installation.

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

1. Insérez et montez le CD-ROM d'installation du Serveur d’installation approprié sur un point de montage.

   Par exemple :

   ```
   mkdir /cdrom
   mount /dev/dsk/c0t0d0 /cdrom
   ```

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

   - Pour copier les répertoires `DP_DEPOT` et `LOCAL_INSTALL` (où se trouvent les fichiers d'installation) sur votre disque local, exécutez la commande suivante :

     ```
     mkdir <répertoire>
     cp -r /cdrom/DP_DEPOT <répertoire>
     cp -r /cdrom/LOCAL_INSTALL <répertoire>
     ```

     Montez le deuxième CD-ROM du Serveur d’installation et copiez aussi tous les fichiers du répertoire `DP_DEPOT` dans le répertoire d'installation :

     ```
     cp -r /cdrom/DP_DEPOT <répertoire>
     ```

- Pour copier l'ensemble du CD-ROM sur votre disque local, exécutez la commande :

  ```
  cp -r /cdrom <rép_image_cd>
  ```

2. Exécutez la commande `omnisetup.sh`.

   Pour lancer cette commande à partir du CD-ROM, saisissez :

   ```
   cd /cdrom/LOCAL_INSTALL
   ./omnisetup.sh -IS1
   ```

   Pour lancer l'installation à partir du disque :

   - Si vous avez copié les répertoires `DP_DEPOT` et `LOCAL_INSTALL` des deux CD-ROM sur votre disque local sous *<répertoire>*, allez sur le répertoire qui contient le fichier `omnisetup.sh` et exécutez la commande suivante :

     ```
     cd <répertoire>/LOCAL_INSTALL
     ./omnisetup.sh -IS1 -IS2
     ```

   - Si vous avez copié l'ensemble du CD-ROM dans *<rép_image_cd>*, exécutez la commande `omnisetup.sh` avec le paramètre `-IS1` :

     ```
     cd <rép_image_cd>/LOCAL_INSTALL
     ./omnisetup.sh -IS1
     ```

3. Si vous réalisez l'installation à partir du CD-ROM monté ou de l'image du CD-ROM, répétez les étapes 1 et 2 avec le deuxième CD-ROM d'installation de Serveur d'installation, mais utilisez le paramètre `omnisetup.sh -IS2` à la place du paramètre `-IS1`.

Installation des clients UNIX à partir de CD-ROM

Limites

L'installation en local des packages UNIX n'est possible *qu'à partir du CD-ROM d'installation du Serveur d'installation HP-UX*. Ceci inclut tous les clients UNIX. En d'autres termes, cela signifie que vous devez utiliser le CD-ROM d'installation du Serveur d'installation HP-UX pour installer le client Solaris ou Linux et non le CD-ROM d'installation du Serveur d'installation Solaris ou Linux.

Procédure d'installation

La procédure d'installation est presque identique à celle décrite pour l'installation du Serveur d'installation UNIX à partir du DVD-ROM, mais une fois l'installation du premier CD-ROM terminée, vous devez insérer le deuxième CD-ROM et lancer une nouvelle fois l'installation.

Pour plus d'informations, reportez-vous à la section “Installation locale de clients UNIX” à la page 130.

Etapes et tâches supplémentaires pour la mise à niveau de Data Protector à partir de CD-ROM

La procédure de mise à niveau de Data Protector à partir de CD-ROM est similaire à la procédure de mise à niveau à partir d'un DVD-ROM.

- ***Sous UNIX***, les packages d'installation sont répartis sur *3 CD-ROM* (un pour le Gestionnaire de cellule et deux pour le Serveur d’installation) ; il est donc nécessaire de lancer les CD-ROM supplémentaires pour poursuivre la mise à niveau.
- ***Sous Windows***, à chaque plate-forme correspond *1 CD-ROM* ; par conséquent, la procédure de mise à niveau Windows à partir d'un CD-ROM est la même qu'à partir d'un DVD-ROM, sauf le chemin d'installation :

  Systèmes 32 bits : `\i386\setup.exe`

  Systèmes 64 bits : `\x8664\setup.exe`

Mise à niveau d'un Gestionnaire de cellule UNIX

Procédez comme suit pour mettre à niveau le Gestionnaire de cellule HP-UX ou Solaris vers Data Protector A.06.00 :

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

   Par exemple :

   ```
   mkdir /cdrom
   mount /dev/c0d0t0 /cdrom
   ```

   Si vous souhaitez installer Data Protector depuis un dépôt sur le disque, procédez comme suit :

   - Copiez les répertoires `DP_DEPOT`, `LOCAL_INSTALL` et `AUTOPASS` (où se trouvent les fichiers d'installation) :

     ```
     mkdir <répertoire>
     cp -r /cdrom/DP_DEPOT <répertoire>
     cp -r /cdrom/AUTOPASS <répertoire>
     cp -r /cdrom/LOCAL_INSTALL <répertoire>
     ```

- Copiez l'ensemble du CD-ROM sur votre disque local :

  ```
  cp -r /cdrom <rép_image_cd>
  ```

2. Exécutez la commande `omnisetup.sh`.

   Pour lancer cette commande à partir du CD-ROM, exécutez :

   ```
   cd /cdrom/LOCAL_INSTALL
   ./omnisetup.sh
   ```

   Pour lancer l'installation à partir du disque :

   - Si vous avez copié les répertoires `DP_DEPOT` et `LOCAL_INSTALL` du CD-ROM sur votre disque local sous *<répertoire>*, allez sur le répertoire qui contient le fichier `omnisetup.sh` et exécutez la commande suivante :

     ```
     cd <répertoire>/LOCAL_INSTALL
     ./omnisetup.sh
     ```

   - Si vous avez copié l'ensemble du CD-ROM dans *<rép_image_cd>*, exécutez la commande `omnisetup.sh` sans paramètres :

     ```
     cd <rép_image_cd>/LOCAL_INSTALL
     ./omnisetup.sh
     ```

3. `omnisetup.sh` vous invite à installer ou à mettre à niveau l'utilitaire HP OpenView AutoPass, si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à la section “Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP OpenView AutoPass” à la page 334. L'installation d'AutoPass est recommandée.

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

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

   Lorsque la version A.05.x de Data Protector est détectée, la procédure de mise à niveau démarre automatiquement. Si vous souhaitez effectuer une installation propre (la version précédente de la base de données sera effacée), désinstallez l'ancienne version puis redémarrez l'installation.

Pour plus de détails sur la gestion des licences, reportez-vous aux sections “Installation d'un Gestionnaire de cellule UNIX” à la page 21 et “Installation des Serveurs d'installation pour UNIX” à la page 40.

4. Si vous réalisez une mise à niveau de Data Protector A.05.00 ou A.05.10 et que la cellule contient des clients Windows, un message vous informera que la conversion des noms de fichier de la base de données IDB va être réalisée. La conversion de la base de données IDB est nécessaire pour la gestion correcte des noms de fichiers comportant des caractères internationaux. Pour plus de détails, reportez-vous à la section “Conversion des noms de fichiers de la base de données IDB” à la page 281.
5. Si le système est doté d'un Serveur d’installation, `omnisetup.sh` vous invite à insérer le CD-ROM d'installation du Serveur d’installation HP-UX ou Solaris approprié pour poursuivre l'installation. Effectuez uniquement les étapes 1 et 2 en utilisant le CD-ROM d'installation du Serveur d’installation HP-UX ou Solaris approprié pour mettre à niveau le Serveur d’installation. Pour obtenir la liste des CD-ROM d'installation de Data Protector, reportez-vous à la section “CD-ROM d'installation Data Protector” à la page C-2.

Mise à niveau d'un Serveur d’installation UNIX

Le Serveur d’installation HP-UX est mis à niveau automatiquement lorsque la commande `omnisetup.sh` est exécutée.

Sous HP-UX, cette commande met automatiquement à niveau le package existant à l'aide de l'utilitaire `swinstall`. Sous Solaris, cette commande supprime l'ensemble des packages existants à l'aide de l'utilitaire `pkgrm` et installe les nouveaux packages à l'aide de l'utilitaire `pkgadd`.

Si le Serveur d’installation est installé avec des composants client, il sera supprimé par la commande `omnisetup.sh`. Dans ce cas, installez un nouveau dépôt de Serveur d’installation au moyen de la commande `omnisetup.sh -IS`, puis réimportez le Serveur d’installation mis à niveau. Pour plus de détails, reportez-vous à la section “Importation d'un Serveur d’installation dans une cellule” à la page 199.

Procédure de mise à niveau

Procédez comme suit pour mettre à niveau le Serveur d’installation HP-UX ou Solaris vers Data Protector A.06.00 :

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

Par exemple :

```
mkdir /cdrom
mount /dev/c0d0t0 /cdrom
```

Si vous souhaitez installer Data Protector depuis un dépôt sur le disque, procédez comme suit :

- Pour copier les répertoires DP_DEPOT et LOCAL_INSTALL (où se trouvent les fichiers d'installation) sur votre disque local, procédez comme suit :

  ```
  mkdir <répertoire>
  cp -r /cdrom/DP_DEPOT <répertoire>
  cp -r /cdrom/LOCAL_INSTALL <répertoire>
  ```

  Montez le deuxième CD-ROM du Serveur d'installation et copiez aussi tous les fichiers du répertoire DP_DEPOT dans le répertoire d'installation :

  ```
  cp -r /cdrom/DP_DEPOT <répertoire>
  ```

- Pour copier l'ensemble du CD-ROM sur votre disque local, exécutez la commande :

  ```
  cp -r /cdrom <rép_image_cd>
  ```

2. Exécutez la commande omnisetup.sh.

   Pour lancer cette commande à partir du CD-ROM, exécutez :

   ```
   cd /cdrom/LOCAL_INSTALL
   ./omnisetup.sh
   ```

   Pour lancer l'installation à partir du disque, effectuez l'une des étapes suivantes :

   - Si vous avez copié les répertoires DP_DEPOT et LOCAL_INSTALL du CD-ROM sur votre disque local sous <répertoire>, allez sur le répertoire qui contient le fichier omnisetup.sh et exécutez la commande suivante :

     ```
     cd <répertoire>/LOCAL_INSTALL
     ./omnisetup.sh
     ```

   - Si vous avez copié l'ensemble du CD-ROM dans <rép_image_cd>, exécutez la commande omnisetup.sh sans paramètres :

     ```
     cd <rép_image_cd>/LOCAL_INSTALL
     ./omnisetup.sh
     ```

3. Si vous avez exécuté `omnisetup.sh` à partir du CD-ROM ou copié le CD-ROM entier sur le disque, répétez la procédure en utilisant le deuxième CD-ROM d'installation du Serveur d’installation.

D

E

W