HP Data Protector 6.20

guide d'installation et de choix des licences

Référence:
Première Édition: Mars 2011

Informations juridiques

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

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

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

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

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

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

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

UNIX® est une marque déposée de The Open Group.

Sommaire

Figures

Tableaux

Historique des publications

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

Tableau 1 Informations sur cette édition

Référence	Edition du guide	Produit
B6960-96002	Juillet 2006	Data Protector Version A.06.00
B6960-96036	Novembre 2008	Data Protector Version A.06.10
B6960-90152	Septembre 2009	Data Protector Version A.06.11
	Mars 2011	Data Protector Version A.06.20

A propos de ce manuel

Ce manuel fournit des informations sur :

- l'installation du produit réseau Data Protector ;
- les conditions à remplir avant de démarrer la procédure d'installation ;
- la mise à niveau et l'attribution de licences.

Public visé

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

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

Documentation

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

Guides

Les guides Data Protector sont disponibles au format PDF. Vous pouvez installer les fichiers PDF lors de l'installation de Data Protector en sélectionnant le composant `Documentation en français (guides, aide)` sous Windows ou le composant `OB2-DOCS` sous UNIX. Les guides sont alors placés dans le répertoire `répertoire_Data_Protector\docs` sous Windows ou `/opt/omni/doc/C/` sous UNIX.

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

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

Dans la section Storage, cliquez sur **Storage Software**, puis sélectionnez votre produit.

- *Guide conceptuel HP Data Protector*

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

- *Guide d'installation et de choix des licences HP Data Protector*

  Ce guide décrit la procédure d'installation de Data Protector en fonction de votre système d'exploitation et de l'architecture de votre environnement. En outre, il contient des informations sur les mises à niveau de Data Protector et sur l'obtention de licences correspondant à votre environnement.

- *Guide de dépannage HP Data Protector*

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

- *Guide de récupération après sinistre HP Data Protector*

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

- *Guide d'intégration HP Data Protector*

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

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

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

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

    Ce guide décrit l'intégration de Data Protector avec Oracle Server, SAP R/3 et SAP MaxDB.

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

    Ce guide décrit l'intégration de Data Protector avec les applications IBM suivantes : Informix Server, IBM DB2 UDB et Lotus Notes/Domino Server.

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

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

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

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

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

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

- *Guide d'intégration HP Data Protector pour HP Operations Manager sous UNIX*

  Ce guide décrit les procédures de surveillance et de gestion de l'état et des performances de l'environnement Data Protector avec HP Operations Manager et HP Service Navigator sous UNIX.

- *Guide d'intégration HP Data Protector pour HP Operations Manager sous Windows*

  Ce guide décrit les procédures de surveillance et de gestion de l'état et des performances de l'environnement Data Protector avec HP Operations Manager sous Windows.

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

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

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

  Ce guide décrit la configuration et l'utilisation de l'intégration de Data Protector avec HP StorageWorks P6000 EVA Disk Array Family, HP StorageWorks P9000 XP Disk Array Family, HP StorageWorks P4000 SAN Solutions, EMC Symmetrix Remote Data Facility et TimeFinder. Il s'adresse aux opérateurs ou aux

administrateurs de sauvegarde. Il décrit la sauvegarde avec temps d'indisponibilité nul, la restauration instantanée, ainsi que la restauration de systèmes de fichier et d'images disque.

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

  Ce guide décrit comment configurer et utiliser Data Protector pour effectuer des sauvegardes avec temps d'indisponibilité nul, des restaurations instantanées ainsi que des restaurations standard de bases de données Oracle Server, SAP R/3, Microsoft Exchange Server et Microsoft SQL Server.

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

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

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

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

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

  Ce guide contient des informations sur le suivi et la gestion des supports de stockage hors ligne à l'intention des administrateurs réseau chargés de la maintenance et de la sauvegarde des systèmes. Il décrit l'installation et la configuration de l'application, la réalisation des opérations quotidiennes relatives aux supports et la production de rapports.

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

  Ce guide fournit une description des nouveautés de HP Data Protector 6.20. Il donne également des informations sur les conditions requises pour l'installation, les correctifs requis et les limitations, ainsi que sur les problèmes connus et leurs solutions.

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

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

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

  Ce guide remplit une fonction similaire pour Media Operations.

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

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

Aide en ligne

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

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

- ***Windows :*** Ouvrez `DP_help.chm`.
- ***UNIX :*** Décompressez le fichier d'archive `DP_help.tar.gz` et accédez au système d'aide en ligne en cliquant sur `DP_help.htm`.

Organisation de la documentation

Abréviations

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

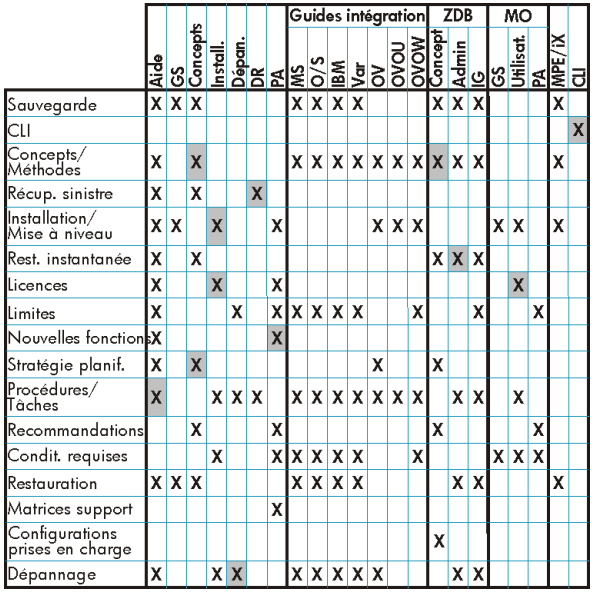
Abréviation	Guide
CLI	Guide de référence de l'interface de ligne de commande
Concepts	Guide conceptuel
DR	Guide de récupération après sinistre
GS	Guide de démarrage rapide
GRE-SPS	Guide d'utilisation de l'extension de restauration granulaire pour Microsoft SharePoint Server

Abréviation	Guide
GRE-VMware	Guide d'utilisation de l'extension de restauration granulaire pour VMware vSphere
Aide	Aide en ligne
IG-IBM	Guide d'intégration pour les applications IBM : Informix, DB2 et Lotus Notes/Domino
IG-MS	Guide d'intégration pour les applications Microsoft : SQL Server, SharePoint Server et Exchange Server
IG-O/S	Guide d'intégration pour Oracle et SAP
IG-OMU	Guide d'intégration pour HP Operations Manager sous UNIX
IG-OMW	Guide d'intégration pour HP Operations Manager sous Windows
IG-Var	Guide d'intégration pour Sybase, Network Node Manager et le serveur NDMP (Network Data Management Protocol)
IG-VirtEnv	Guide d'intégration pour les environnements de virtualisation : VMware, Microsoft Hyper-V et Citrix XEN Server
IG-VSS	Guide d'intégration pour Microsoft Volume Shadow Copy Service
installation	Guide d'installation et de choix des licences
MO GS	Guide de démarrage Media Operations
MO RN	Références, notes de publication et annonces produits Media Operations
MO UG	Guide de l'utilisateur Media Operations
PA	Références, notes de publication et annonces produits
Dépan.	Guide de dépannage
ZDB Admin	Guide de l'administrateur ZDB
Concept ZDB	Guide conceptuel ZDB

Abréviation	Guide
ZDB IG	Guide d'intégration ZDB

Organisation

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



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

Intégrations

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

Application logicielle	Guides
HP Network Node Manager (NNM)	IG-Var
HP Operations Manager	IG-OMU, IG-OMW
IBM DB2 UDB	IG-IBM

Application logicielle	Guides
Informix Server	IG-IBM
Lotus Notes/Domino Server	IG-IBM
Media Operations	Utilisateur MO
Microsoft Exchange Server	IG-MS, ZDB IG
Microsoft Hyper-V	IG-VirtEnv
Microsoft SharePoint Server	IG-MS, ZDB IG, GRE-SPS
Microsoft SQL Server	IG-MS, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-VSS
Serveur NDMP (Network Data Management Protocol)	IG-Var
Oracle Server	IG-O/S, ZDB IG
SAP MaxDB	IG-O/S
SAP R/3	IG-O/S, ZDB IG
Sybase Server	IG-Var
VMware vSphere	IG-VirtEnv, GRE-VMware

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

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

Famille de baies de disques	Guides
HP StorageWorks P9000 XP Disk Array Family	Tous les guides ZDB

Conventions typographiques et symboles

Tableau 2 Conventions typographiques

Convention	Elément
Texte bleu : Tableau 2 à la page 27	Renvois et adresses électroniques
Texte souligné en bleu : http://www.hp.com	Adresses de sites Web
Texte *italique*	Texte mis en évidence
Texte `non proportionnel`	• Noms des fichiers et des répertoires • Sortie du système • Code • Commandes et leurs arguments, valeurs des arguments
Texte *`non proportionnel, italique`*	• Variables de code • Variables de commande
Texte **`non proportionnel, gras`**	Texte à espacement fixe et mis en évidence

△ ATTENTION :

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

IMPORTANT :

Fournit des explications ou des instructions spécifiques.

REMARQUE :

Fournit des informations complémentaires.

CONSEIL :

Propose des conseils utiles et des raccourcis.

Interface utilisateur graphique de Data Protector

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

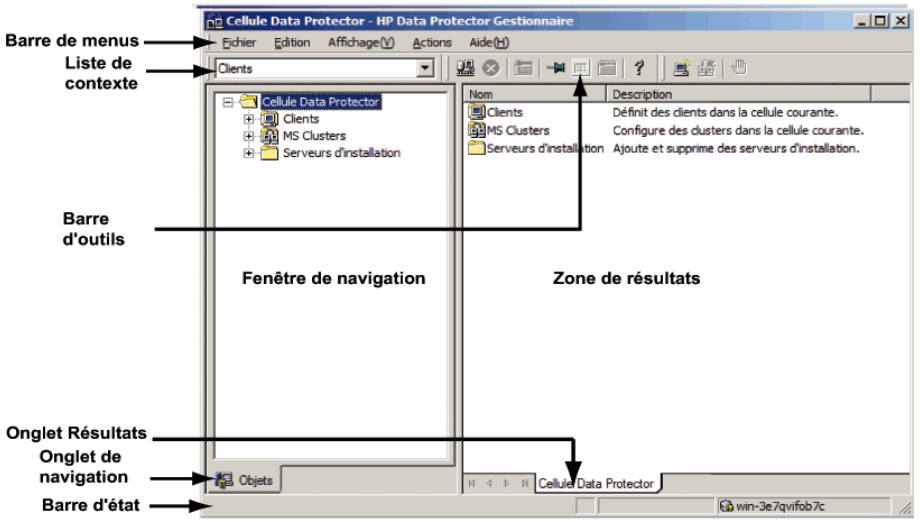


Figure 1 Interface utilisateur graphique de Data Protector

Informations générales

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

Assistance technique HP

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

http://www.hp.com/support

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

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

Service d'enregistrement

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

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

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

Sites Web HP :

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

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

Vos commentaires sur la documentation

HP souhaite connaître votre opinion.

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

1 Présentation de la procédure d'installation

Dans ce chapitre

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

Présentation de la procédure d'installation

Un environnement de sauvegarde Data Protector est un ensemble de systèmes doté d'une stratégie de sauvegarde commune dans le même fuseau horaire et sur le même LAN/SAN. Cet environnement réseau est appelé **cellule** Data Protector. Une cellule type se compose d'un Gestionnaire de cellule, de plusieurs Serveurs 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 interne assure le suivi des fichiers sauvegardés et de la configuration de la cellule.

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

Une cellule comprend généralement un Gestionnaire de cellule et plusieurs clients. Un système informatique devient un **client** Data Protector dès que l'un des composants logiciels Data Protector est installé sur le système. L'installation de composants clients sur un système dépend du rôle de ce dernier dans votre environnement de sauvegarde. Les composants Data Protector peuvent être installés en local sur un seul système ou sur plusieurs systèmes à partir de Serveur 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 utilisateur graphique (GUI) et une interface de ligne de commande (CLI).

Sur les systèmes clients dont les disques sont à sauvegarder, des composants **Agent de disque** Data Protector doivent être installés. L'Agent de disque vous permet de sauvegarder des données à partir du disque client ou de les restaurer.

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

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

- Le système sur lequel le Gestionnaire de cellule sera installé. Pour connaître les systèmes d'exploitation et les versions pris en charge, reportez-vous aux dernières matrices de support à l'adresse http://www.hp.com/support/manuals.

  Il ne peut y avoir qu'un seul Gestionnaire de cellule par cellule. L'exécution de Data Protector exige qu'un Gestionnaire de cellule soit installé.
- Les systèmes qui seront utilisés pour accéder aux fonctions de Data Protector via l'interface utilisateur, et qui doivent être dotés du composant Interface utilisateur.
- Les systèmes qui seront sauvegardés et qui doivent être équipés du composant Agent de disque pour la sauvegarde des systèmes de fichiers et du composant Agent d'application pertinent pour les intégrations de bases de données en ligne.
- Les systèmes auxquels les périphériques de sauvegarde seront connectés et qui requièrent un composant Agent de support.
- Le ou les systèmes sur lesquels le ou les serveurs d'installation Data Protector seront installés. Deux types de serveurs d'installation (IS) sont disponibles pour l'installation des logiciels distants : l'un pour les clients UNIX et l'autre pour les clients Windows.

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

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

REMARQUE :

Le Serveur d'installation pour Windows doit être installé sur un système Windows. Le Serveur d'installation pour UNIX doit être installé sur un système HP-UX, Solaris ou Linux. Pour connaître les versions du système d'exploitation prises en charge, reportez-vous aux dernières matrices de support à l'adresse http://www.hp.com/support/manuals.

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 Serveur d'installation et de l'interface utilisateur.
4. Installation des systèmes clients, soit à distance (option recommandée, si possible), soit en local à partir du DVD-ROM d'installation.

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 clients Windows XP Edition familiale, Novell NetWare et HP OpenVMS. Ceux-ci doivent être installés localement.

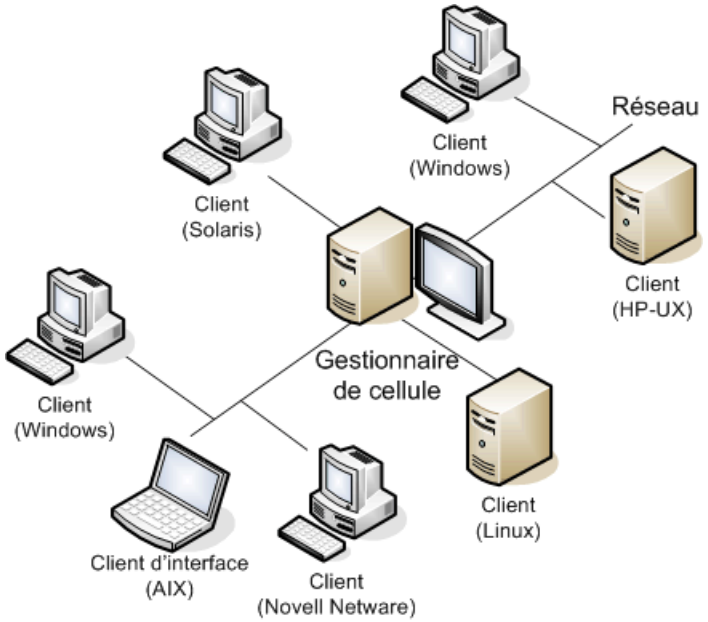


Figure 2 Cellule Data Protector

Concept d'installation à distance

Une fois que vous avez installé le Gestionnaire de cellule Data Protector, l'interface utilisateur et le Serveur d'installation (au moins un Serveur d'installation est nécessaire pour chaque plate-forme, UNIX et Windows), vous pouvez distribuer le logiciel Data Protector aux clients à l'aide des systèmes d'exploitation prenant en charge l'installation à distance. Reportez-vous à la Figure 3 à la page 36.

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

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

Les systèmes clients sous Windows XP Edition familiale doivent être installés en local à partir du DVD-ROM d'installation de Data Protector pour Windows.

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

Le logiciel client peut être installé à distance sur les systèmes d'exploitation UNIX pris en charge, tels que HP-UX, Solaris, Linux et AIX, à partir d'un Serveur d'installation pour UNIX. Pour obtenir la liste des périphériques pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

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

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

Pour plus d'informations sur les méthodes d'installation disponibles pour les différents clients Data Protector, reportez-vous à la section “Installation des clients Data Protector” à la page 72.

Pour connaître la procédure de désinstallation locale des clients UNIX, reportez-vous à la section “Installation en local de clients UNIX et Mac OS X” à la page 151.

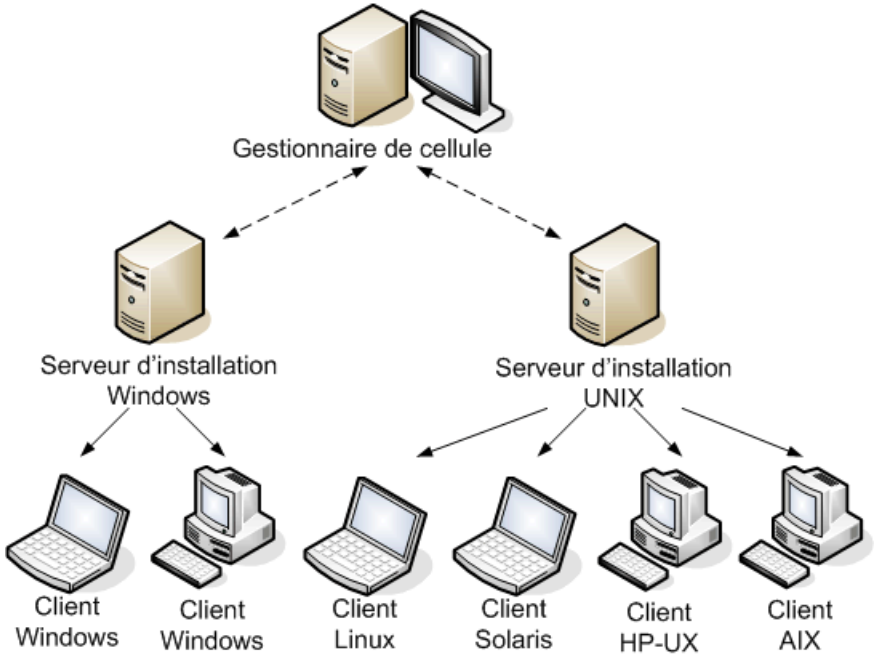


Figure 3 Concept d'installation de Data Protector

DVD-ROM d'installation de Data Protector

Data Protector prend en charge différents systèmes d'exploitation sur plusieurs architectures de processeur. Par conséquent, trois DVD-ROM sont nécessaires pour couvrir toutes les plates-formes. Le Tableau 3 à la page 37 indique les composants disponibles sur les DVD-ROM.

REMARQUE :

Les fichiers d'installation Data Protector pour les systèmes d'exploitation Windows Vista, Windows 7 et Windows Server 2008 sont dotés de la signature numérique de HP.

Tableau 3 Liste des DVD-ROM Data Protector

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

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

[1]HP AutoPass n'est pas disponible pour les systèmes d'exploitation Windows Server 2003 x64, Windows Vista x64 et Windows Server 2008 x64.

[2]HP AutoPass n'est pas disponible pour Linux.

Choix du système Gestionnaire de cellule

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

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

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

- Plates-formes prises en charge

  Vous pouvez installer le Gestionnaire de cellule sur les plates-formes Windows, HP-UX, Solaris et Linux. Pour plus de détails sur les versions prises en charge sur ces plates-formes, consultez les dernières matrices de support à l'adresse http://www.hp.com/support/manuals.

- Fiabilité du système Gestionnaire de cellule

  Dans la mesure où le Gestionnaire de cellule contient la base de données IDB et où la sauvegarde et la restauration sont impossibles en cas de mauvais

fonctionnement 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 requis

  Le Gestionnaire de cellule contient la base de données interne (IDB) de Data Protector. La base de données interne contient des informations concernant les données sauvegardées et leurs supports, messages de session et périphériques. En fonction de votre environnement, la base peut atteindre une taille significative. Par exemple, si la majorité des sauvegardes concerne des systèmes de fichiers, la base IDB représenterait généralement 2 % de l'espace disque occupé par les données sauvegardées. Vous pouvez utiliser le tableau `IDB_capacity_planning.xls` (présent sur tous les DVD-ROM d'installation de Data Protector) pour estimer la taille de la base de données IDB.

  Pour plus d'informations sur la planification et la gestion de la taille et de la croissance de la base de données, recherchez l'entrée suivante dans l'index de l'aide en ligne : “croissance et performances de l'IDB“.

  Pour connaître l'espace disque minimum nécessaire, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

REMARQUE :

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

Etape suivante

Pour connaître la configuration minimale requise de votre futur système Gestionnaire de cellule, reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector” à la page 44.

Choix du système de l'interface utilisateur de Data Protector

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

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

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

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

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

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

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

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

Interface utilisateur graphique de Data Protector

L'interface utilisateur graphique 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**, **Opérations sur les objets**, **Rapports**, **Moniteur**, **Restauration instantanée** et **Base de données interne**, lesquelles vous permettent d'exécuter toutes les tâches associées.

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

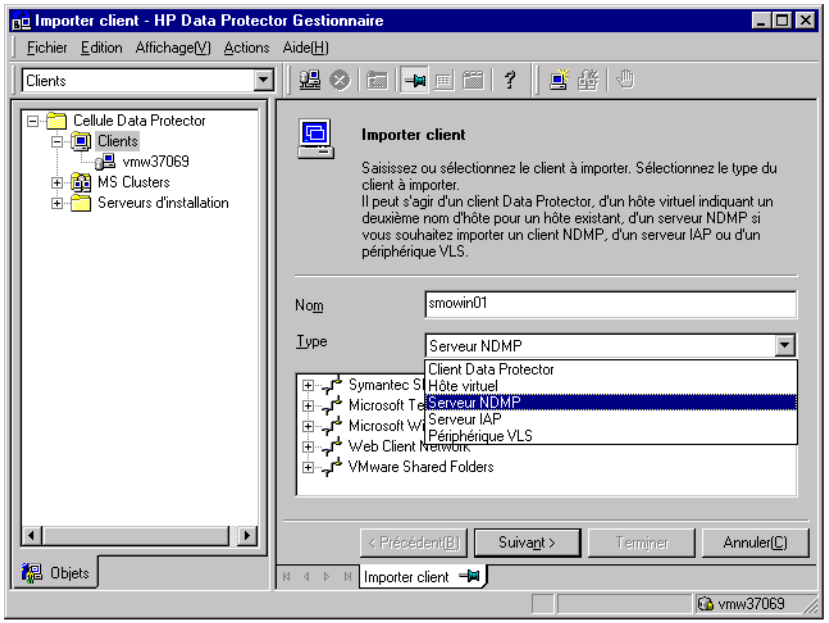


Figure 4 Interface utilisateur graphique de Data Protector

Reportez-vous également à la Figure 1 à la page 29 de la préface, qui définit les principales zones de l'interface utilisateur de Data Protector.

REMARQUE :

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

2 Installation de Data Protector sur votre réseau

Dans ce 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 44.
- Installation des clients Data Protector. Reportez-vous à la section "Installation des clients Data Protector" à la page 72.
- Installation des clients d'intégration Data Protector. Reportez-vous à la section "Installation des clients d'intégration Data Protector" à la page 157.
- Installation de l'interface utilisateur Data Protector localisée. Reportez-vous à la section "Installation de l'interface utilisateur localisée de Data Protector" à la page 195.
- 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 200.
- Installation du composant Rapports Web Data Protector. Reportez-vous à la section "Installation des Rapports Web de Data Protector" à la page 201.
- Installation de Data Protector sur MC/ServiceGuard. Reportez-vous à la section "Installation de Data Protector sur MC/ServiceGuard" à la page 203.
- Installation de Data Protector sur Microsoft Cluster Server. Reportez-vous à la section "Installation de Data Protector sur Microsoft Cluster Server" à la page 204.
- 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 216.
- 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 217.

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

Pour connaître le déroulement de la procédure d'installation, reportez-vous à la Figure 5 à la page 44:

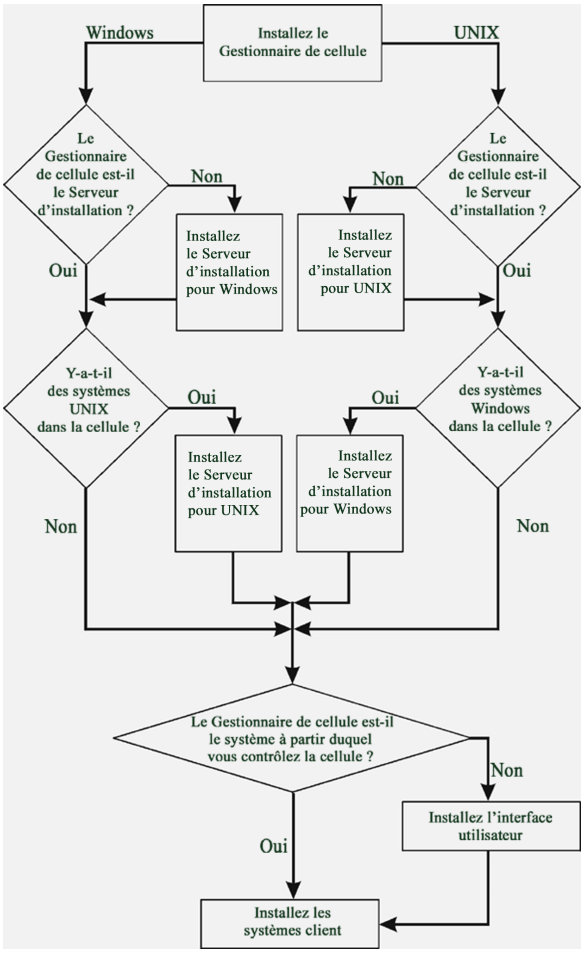


Figure 5 Procédure d'installation

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

IMPORTANT :

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

Installation d'un Gestionnaire de cellule UNIX

Cette section fournit des instructions détaillées sur la procédure d'installation d'un Gestionnaire de cellule UNIX. Si vous souhaitez n'installer que le Gestionnaire de cellule Windows, reportez-vous à la section “Installation d'un Gestionnaire de cellule Windows” à la page 55.

Configuration système requise

- Le système HP-UX, Solaris ou Linux qui deviendra le Gestionnaire de cellule doit :
  - Disposer d'un espace disque suffisant pour le logiciel Data Protector. Pour plus d'informations à ce sujet, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*. Pour surmonter les problèmes de manque d'espace, vous pouvez effectuer l'installation sur des répertoires liés ; reportez-vous au préalable aux sections “Structure des répertoires installés sous HP-UX, Solaris et Linux” à la page 50 et “Allocation d'espace disque supplémentaire pour l'installation du Gestionnaire de cellule” à la page 54.
  - Disposer d'un espace disque suffisant (équivalent à environ 2 % des données à sauvegarder) pour la base de données IDB. Pour plus de détails à ce sujet, reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector*. Notez que la conception actuelle de la base de données IDB permet de déplacer les fichiers binaires si la croissance de la base de données rend cette opération nécessaire. Dans l'index de l'aide en ligne, recherchez : "base de données interne (IDB), calcul de la taille".
  - Prendre en charge les noms de fichiers longs. Pour vérifier si votre système de fichiers prend en charge les noms de fichiers longs, utilisez la commande `getconf NAME_MAX répertoire`.
  - Inclure un démon `inetd` ou `xinetd` opérationnel.

- Disposer du port numéro 5555 (par défaut). Si ce n'est pas le cas, reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 414.
- 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 421.
- Pour installer le serveur d'interface utilisateur graphique Java ou le client d'interface graphique Java, veillez à ce que le numéro de port 5556 soit libre.
- Pour le client d'interface Java, une version prise en charge de l'environnement JRE (Java Runtime Environment) est nécessaire. Reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector* ou aux dernières matrices de support à l'adresse http://www.hp.com/support/manuals.

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

REMARQUE :

Sur les plates-formes Gestionnaire de cellule qui ne prennent pas en charge l'interface utilisateur graphique d'origine de Data Protector, vous pouvez utiliser l'interface utilisateur graphique Java de Data Protector ou installer l'interface utilisateur graphique d'origine de Data Protector sur un système qui la prend en charge. Utilisez la commande `omniusers` pour créer un compte utilisateur distant sur le nouveau Gestionnaire de cellule. Vous pouvez alors utiliser ce compte utilisateur avec l'interface utilisateur graphique 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 203.

REMARQUE :

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

Recommandation

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

Définition des paramètres de noyau

Sous HP-UX, il est recommandé de régler le paramètre de noyau `maxdsiz` (taille maximale des segments de données) ou `maxdsiz_64` (pour les systèmes 64 bits) sur au moins 134 217 728 octets (128 Mo), et le paramètre de noyau `semmnu` (nombre de structures Undo de sémaphore) sur au moins 256 Mo. Une fois ces modifications effectuées, recompilez le noyau et redémarrez la machine.

Sous Solaris, il est recommandé de définir le paramètre de noyau `shmsys:shminfo_shmmax` (taille maximale du segment de mémoire partagée (SHMMAX)) dans `/etc/system` à 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 *Guide de référence de l'interface de ligne de commande HP Data Protector* se trouvant dans le répertoire `point_de_montage/DOCS/C/MAN` sur le DVD-ROM.

Pour installer le Gestionnaire de cellule sur un système HP-UX, Solaris ou Linux, procédez comme suit :

1. Insérez et montez le DVD-ROM d'installation HP-UX, ou Solaris et Linux 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 le répertoire où se trouvent les fichiers d'installation sur votre disque local, exécutez la commande suivante :

     ```
     mkdir répertoire
     cp -r /dvdrom/rép_plateforme/DP_DEPOT répertoire
     cp -r /dvdrom/LOCAL_INSTALL répertoire
     ```

     Où *rép_plateforme* est :

`hpux`	Systèmes HP-UX
`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 suivante :

     `cp -r /dvdrom` *`rép_image_dvd`*

2. Exécutez la commande `omnisetup.sh`.

   Pour exécuter 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 d'installation dans *`le répertoire`* de votre disque local, exécutez la commande suivante :

     ```
     cd répertoire/LOCAL_INSTALL
     ./omnisetup.sh -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 AutoPass si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement par Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à la section "Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass" à la page 348 et à l'aide en ligne HP AutoPass. L'installation d'AutoPass est recommandée.

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

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

   Sous Linux, HP AutoPass n'est pas installé.

REMARQUE :

Si vous avez installé le Gestionnaire de cellule sous Solaris 9 ou 10, installez l'Agent de disque à distance sur le Gestionnaire de cellule après l'installation à l'aide d'un Serveur d'installation. L'Agent de disque Solaris générique sera ainsi remplacé par l'Agent de disque Solaris 9 ou Solaris 10. Sous Solaris 10, l'installation à distance de l'Agent de support sur le Gestionnaire de cellule s'avère également nécessaire. Reportez-vous à la section "Installation distante de clients Data Protector" à la page 83 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 64.

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 54.

`/opt/omni/bin`	Toutes les commandes
`/opt/omni/help/C`	Fichiers d'aide en ligne

`/opt/omni/lbin`	Commandes internes de Data Protector
`/opt/omni/sbin`	Commandes super-utilisateur
`/opt/omni/sbin/install`	Scripts d'installation
`/etc/opt/omni`	Informations de configuration
`/opt/omni/lib`	Bibliothèques partagées pour la compression, le codage de données et la gestion de périphériques
`/opt/omni/doc/C`	Guides au format PDF électronique (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. Reportez-vous à l'index de l'aide en ligne : "IDB, emplacement des répertoires".
`/opt/omni/java/server`	Répertoire contenant les fichiers exécutables du serveur d'interface utilisateur graphique Java
`/opt/omni/java/client`	Répertoire contenant les fichiers exécutables du client d'interface utilisateur graphique Java

Configuration du démarrage et de l'arrêt automatiques

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

Les fichiers suivants sont configurés automatiquement :

HP-UX :

`/sbin/init.d/omni`

Script contenant les procédures de démarrage et d'arrêt.

`/sbin/rc1.d/K162omni`

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

`/sbin/rc2.d/S838omni`

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

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

Contient une variable `omni` définissant :

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

Solaris :

`/etc/init.d/omni`

Script contenant les procédures de démarrage et d'arrêt.

`/etc/rc1.d/K09omni`

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

`/etc/rc2.d/S97omni`

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

Linux :

`/etc/init.d/omni`

Script contenant les procédures de démarrage et d'arrêt.

`/etc/rcniveau_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/rcniveau_init.d/S90omni`

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

Où *niveau_init* est égal à 2,3,4 ou 5.

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

HP-UX :

`/etc/services`

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

`/opt/omni/lbin/crs`

Le service CRS de Data Protector est ajouté.

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

`/opt/omni/lbin/crs`

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

`/opt/omni/lbin/rds`

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

`/opt/omni/lbin/mmd`

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

`/opt/omni/lbin/inetd`

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

`/opt/omni/lbin/kms`

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

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

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

Configuration des variables d'environnement

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

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

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

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

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

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

REMARQUE :

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

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

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

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

Etape suivante

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

1. Si vous n'avez pas installé un Serveur d'installation pour UNIX sur le même système, reportez-vous à la section "Installation des Serveurs d'installation pour UNIX" à la page 64.
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 68.
3. Distribuez le logiciel aux clients. Reportez-vous à la section "Installation des clients Data Protector" à la page 72.

Installation d'un Gestionnaire de cellule Windows

Configuration système requise

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

- Etre doté d'une version du système d'exploitation Windows prise en charge. Reportez-vous au site http://www.hp.com/support/manuals pour connaître les systèmes d'exploitation pris en charge pour le Gestionnaire de cellule.
- Disposer de Microsoft Internet Explorer 5.0 ou supérieur.
- Disposer d'un espace disque suffisant pour le logiciel Gestionnaire de cellule de Data Protector. Pour plus d'informations à ce sujet, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Disposer d'un espace disque suffisant (équivalent à environ 2 % des données sauvegardées) pour la base de données IDB. Pour plus d'informations, consultez les *Références, notes de publication et annonces produits HP Data Protector*.
- Disposer du port numéro 5555 (par défaut). Si ce n'est pas le cas, reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 414.
- Disposer d'une adresse IP fixe pour le système sur lequel le Gestionnaire de cellule doit être installé. Si le système est configuré comme client DHCP, son adresse IP change ; vous devez par conséquent soit attribuer une entrée DNS permanente

au système (et le reconfigurer), soit configurer un serveur DHCP de sorte qu'il réserve une adresse IP statique 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.
- Avoir accès à un lecteur de DVD-ROM.
- Pour installer le serveur d'interface utilisateur graphique Java ou le client d'interface graphique Java, veillez à ce que le numéro de port 5556 soit libre.
- Pour le client d'interface Java, une version prise en charge de l'environnement JRE (Java Runtime Environment) est nécessaire. Reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector* ou aux dernières matrices de support à l'adresse http://www.hp.com/support/manuals.
- Vérifiez que les droits d'accès au réseau sont définis sous la règle de sécurité locale Windows pour le compte qui procède à l'installation.

Client Microsoft Terminal Services

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

Recommandation

- Vérifiez si vous avez Microsoft Installer (MSI) 2.0 avant d'installer Data Protector 6.20. 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 6.20.
- Si vous prévoyez que la taille des fichiers binaires DC dépassera 2 Go (elle n'est limitée que par les paramètres du système de fichiers), nous vous conseillons d'utiliser le système de fichiers NTFS.

Gestionnaire de cellule compatible cluster

D'autres conditions et étapes sont requises pour l'installation d'un Gestionnaire de cellule compatible cluster. Reportez-vous à la section “Installation d'un Gestionnaire de cellule compatible cluster” à la page 205.

Procédure d'installation

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

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

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

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

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

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

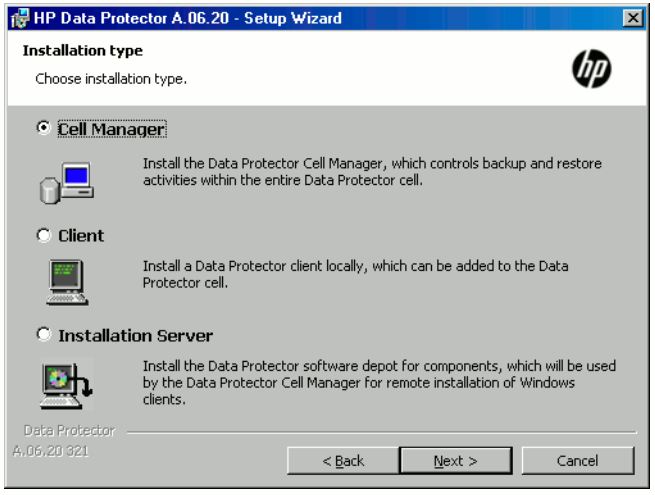


Figure 6 Sélection du type d'installation

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

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

   Pour entrer un autre chemin, cliquez sur **Changer** afin d'ouvrir la fenêtre Changer le dossier de destination actuel.

7. Dans la page Sélection des composants, sélectionnez les composants à installer. Pour obtenir la liste et les descriptions des composants Data Protector, reportez-vous à la section "Composants Data Protector" à la page 77.

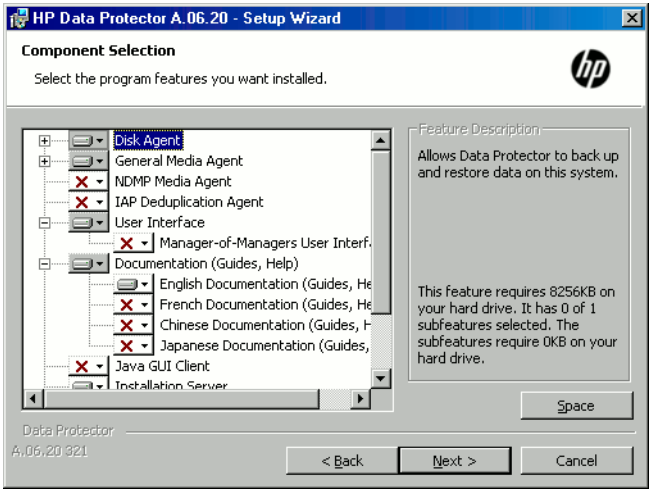


Figure 7 Sélection des composants logiciels

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

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

   Cliquez sur **Suivant**.

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

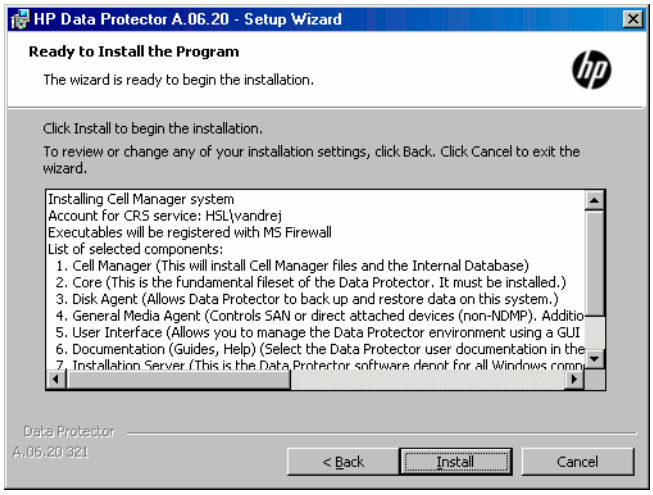


Figure 8 Liste des composants sélectionnés

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

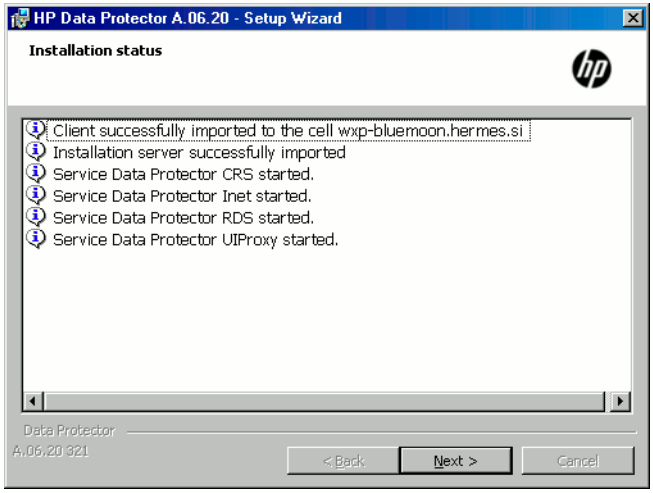


Figure 9 Page d'état de l'installation

11. L'assistant d'installation vous permet d'installer ou de mettre à niveau l'utilitaire HP AutoPass si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à la section "Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass" à la page 348 et à l'aide en ligne HP AutoPass.

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

    HP AutoPass n'est pas installé sur les systèmes Windows Server 2003 x64, Windows Vista x64 et Windows Server 2008 x64.

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

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

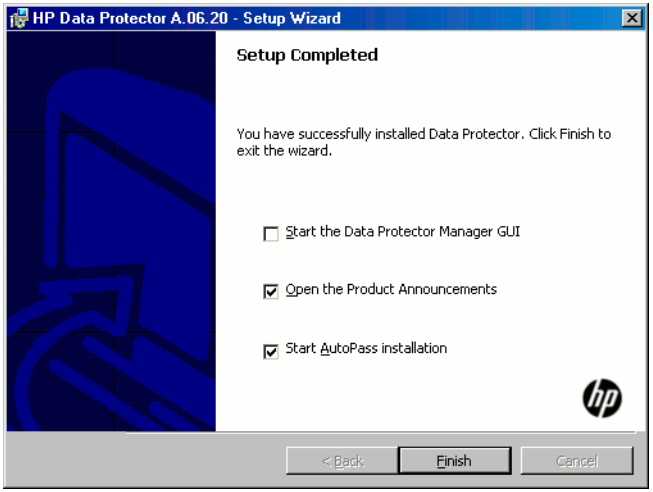


Figure 10 Sélection d'AutoPass pour l'installation

Cliquez sur **Terminer**.

Après l'installation

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

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

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

`crs.exe`	Le service Cell Request Server (CRS) Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Il lance et contrôle les sessions de sauvegarde et de restauration dans la cellule. Il s'exécute dans le répertoire `répertoire_Data_Protector\bin`.
`rds.exe`	Le service Raima Database Server (RDS) Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Le RDS gère l'IDB (base de données interne). Il s'exécute dans le répertoire `répertoire_Data_Protector\bin`.
`mmd.exe`	Le service Media Management Daemon (MMD) de Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Il gère les opérations de gestion des périphériques et des supports. Il s'exécute dans le répertoire `répertoire_Data_Protector\bin`.

`omniinet.exe`	Le service du client Data Protector qui permet au Gestionnaire de cellule de démarrer des agents sur d'autres systèmes. Le service `Inet Data Protector` doit s'exécuter sur tous les systèmes de la cellule Data Protector. Il s'exécute dans le répertoire `répertoire_Data_Protector\bin`.
`kms.exe`	Le service du serveur gestionnaire de clés (KMS) de Data Protector s'exécute sur le système du Gestionnaire de cellule et est lancé lorsque le logiciel du Gestionnaire de cellule est installé sur le système. Ce service gère les clés pour la fonction de cryptage de Data Protector. Il s'exécute dans le répertoire `répertoire_Data_Protector\bin`.
`uiproxy.exe`	Le serveur d'interface utilisateur graphique Java de Data Protector (service `UIProxy`) s'exécute sur le système du Gestionnaire de cellule dans le répertoire `répertoire_Data_Protector\java\server\bin`. Le service `UIProxy` est chargé de la communication entre le client de l'interface Java et le Gestionnaire de cellule.

REMARQUE :

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

CONSEIL :

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

Dépannage

Si l'installation a échoué, contrôlez la configuration vérifiée par le `processus d'installation` lui-même, et essayez de déterminer les causes de l'échec si la configuration n'a pas été respectée. Reportez-vous à la section Configuration système requise à la page 55.

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

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

Etape suivante

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

1. Installez le Serveur d'installation pour UNIX, si votre environnement de sauvegarde est mixte. Reportez-vous à la section “Installation des Serveurs d'installation” à la page 63. 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 72.

Installation des Serveurs d'installation

Les Serveurs d'installation peuvent être installés sur le système du Gestionnaire de cellule ou sur tout système pris en charge et connecté au Gestionnaire de cellule par un réseau local. Reportez-vous au site http://www.hp.com/support/manuals pour connaître les systèmes d'exploitation pris en charge pour le Serveur d'installation.

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

Installation des Serveurs d'installation pour UNIX

Configuration système requise

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

- Disposer du système d'exploitation HP-UX, Solaris ou Linux. Pour obtenir des informations sur les systèmes d'exploitation pris en charge pour le Serveur d'installation, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Inclure un démon `inetd` ou `xinetd` opérationnel.
- Disposer du port numéro 5555 (par défaut). Si ce n'est pas le cas, reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 414.
- Disposer du protocole TCP/IP, lequel doit être en cours d'exécution. Ce protocole doit pouvoir résoudre les noms d'hôte.
- Disposer d'un espace disque suffisant pour l'intégralité du dépôt de logiciel de Data Protector. Pour plus de détails à ce sujet, reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector*.
- Disposer d'un lecteur de DVD-ROM.
- Le Gestionnaire de cellule de la cellule Data Protector doit être mis à niveau vers la version 6.20.

IMPORTANT :

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

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

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

REMARQUE :

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

Procédure d'installation

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

1. Insérez et montez le DVD-ROM d'installation HP-UX, ou Solaris et Linux 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 le répertoire où se trouvent les fichiers d'installation sur votre disque local, exécutez la commande suivante :

     ```
     mkdir répertoire
     cp -r /dvdrom/rép_plateforme/DP_DEPOT répertoire
     cp -r /dvdrom/LOCAL_INSTALL répertoire
     ```

     Où *rép_plateforme* correspond à :

`hpux`	Systèmes HP-UX
`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 suivante :

     ```
     cp -r /dvdrom rép_image_dvd
     ```

2. Exécutez la commande `omnisetup.sh`.

   Pour exécuter 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 d'installation dans *`le répertoire`* de votre disque local, exécutez la commande suivante :

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

   - 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 -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 *Guide de référence de l'interface de ligne de commande HP Data Protector* se trouvant dans le répertoire `point_de_montage/DOCS/C/MAN` sur le DVD-ROM.

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

La commande `omnisetup.sh` installe le Serveur d'installation avec tous les packages. Pour installer certains packages uniquement, utilisez la commande `swinstall` (HP-UX), `pkgadd` (Solaris) ou `rpm` (Linux). Reportez-vous à la section "Installation sur des systèmes HP-UX, Solaris et Linux à l'aide d'outils natifs" à la page 387.

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 HP-UX, ou Solaris et Linux.

REMARQUE :

Si vous installez le composant Interface utilisateur (interface utilisateur graphique ou interface de ligne de commande), mettez à jour au préalable les variables d'environnement. Pour plus d'informations, reportez-vous à la section "Configuration des variables d'environnement" à la page 54.

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

Etape suivante

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

1. Si vous avez installé le Serveur d'installation sur un système autre que celui du Gestionnaire de cellule, il faut ajouter (importer) manuellement le système dans la cellule Data Protector. Reportez-vous à la section "Importation d'un serveur d'installation dans une cellule " à la page 224.

   REMARQUE :

   Lorsqu'un Serveur d'installation est importé, le fichier `/etc/opt/omni/server/cell/installation_servers` sur le Gestionnaire de cellule est mis à jour pour que les paquets d'installation à distance installés y figurent. Ce fichier peut être utilisé à partir de l'interface de ligne de commande pour vérifier les paquets d'installation à distance disponibles. Pour maintenir ce fichier à jour, vous devrez exporter, puis réimporter un Serveur d'installation à chaque installation ou suppression d'un paquet d'installation à distance. 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 68.
3. Distribuez le logiciel aux clients. Reportez-vous à la section "Installation des clients Data Protector" à la page 72.

Installation d'un Serveur d'installation pour Windows

Configuration système requise

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

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

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 6.20, 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 6.20.

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 92.

Procédure d'installation

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

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

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

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

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

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

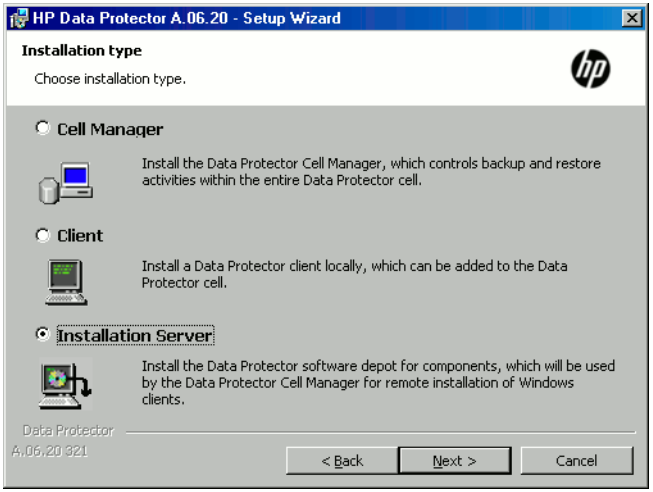


Figure 11 Sélection du type d'installation

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

   Pour entrer un autre chemin, cliquez sur **Changer** afin d'ouvrir la fenêtre Changer le dossier de destination actuel.

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

   Cliquez sur **Suivant**.

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

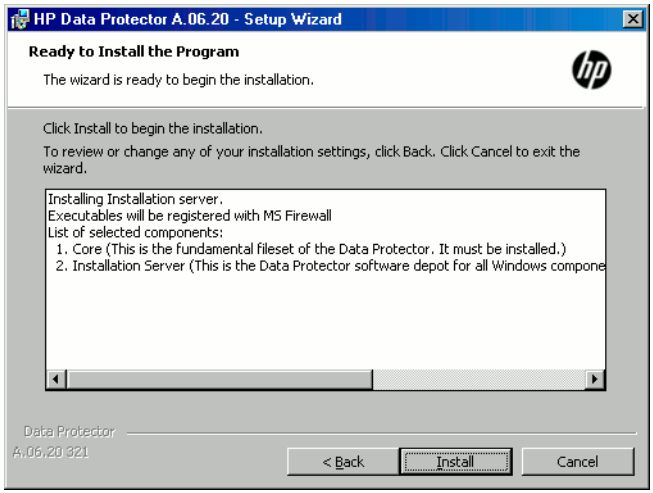


Figure 12 Page de résumé des composants sélectionnés

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

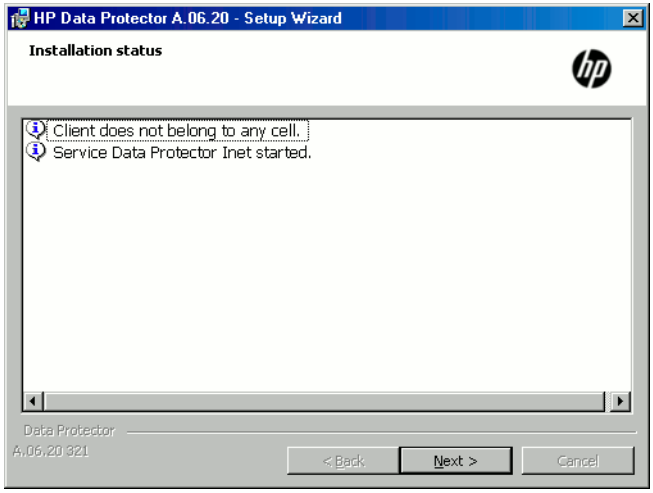


Figure 13 Page d'état de l'installation

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

   Cliquez sur **Terminer**.

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

Etape suivante

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

1. Si vous avez configuré un Serveur d'installation indépendant (ne figurant pas dans le Gestionnaire de cellule, par exemple), vous devez 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 224.
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 64.
3. Distribuez le logiciel aux clients. Reportez-vous à la section “Installation des clients Data Protector” à la page 72.

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 *en local* à partir du DVD-ROM d'installation approprié.

Pour obtenir la liste des DVD-ROM d'installation Data Protector, reportez-vous à la section “DVD-ROM d'installation de Data Protector” à la page 36.

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 377. Pour plus d'informations sur la sécurité, reportez-vous à la section “A propos de la sécurité” à la page 231.

La section “Installation des clients Data Protector” à la page 72 répertorie les systèmes clients Data Protector et contient des références permettant d'accéder à des descriptions détaillées.

Tableau 4 Installation des systèmes clients Data Protector

Système client	Type d'installation et référence
Windows	Installation à distance et en local, voir “Installation de clients Windows” à la page 92.
HP-UX	Installation à distance et en local, voir “Installation de clients HP-UX” à la page 99.
Solaris	Installation à distance et en local, voir “Installation de clients Solaris” à la page 103.
Linux	Installation à distance et en local, voir “Installation de clients Linux” à la page 110.
ESX Server	Installation à distance et en local, voir “Installation des clients ESX Server” à la page 116.
Mac OS X	Installation à distance et en local, voir “Installation des clients Mac OS X” à la page 116.
AIX	Installation à distance et en local, voir “Installation de clients AIX” à la page 117.
Tru64	Installation à distance et en local, voir “Installation de clients Tru64” à la page 120.
SCO	Installation à distance et en local, voir “Installation de clients SCO” à la page 121.
client DAS	Installation à distance et en local, voir “Installation d'un Agent de support pour l'utilisation de la bibliothèque ADIC/GRAU ou de la bibliothèque StorageTek” à la page 124.
client ACS	Installation à distance et en local, voir “Installation d'un Agent de support pour l'utilisation de la bibliothèque ADIC/GRAU ou de la bibliothèque StorageTek” à la page 124.
Novell NetWare	Installation en local, voir “Installation en local de clients Novell NetWare” à la page 134.

Système client	Type d'installation et référence
HP OpenVMS	Installation en local, voir "Installation locale de clients HP OpenVMS" à la page 142.
Autres clients UNIX	Installation en local, voir "Installation en local de clients UNIX et Mac OS X" à la page 151.

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` pour la sauvegarde de la base de données Microsoft Exchange Server, le composant `Intégration Oracle` pour la sauvegarde de la base de données Oracle, etc.). Pour connaître les références, reportez-vous au Tableau 5 à la page 74.

Tableau 5 Installation d'intégrations

Application ou famille de baies de disques	Référence
Microsoft Exchange Server	Reportez-vous à la section "Clients Microsoft Exchange Server" à la page 160.
Microsoft SQL Server	Reportez-vous à la section "Clients Microsoft SQL Server" à la page 162.
Microsoft SharePoint Server	Reportez-vous à la section "Clients Microsoft SharePoint Server" à la page 163.
Microsoft Hyper-V	Reportez-vous à la section "Clients Microsoft Hyper-V" à la page 170.
Sybase Server	Reportez-vous à la section "Clients Sybase" à la page 165.
Informix Server	Reportez-vous à la section "Clients Informix Server" à la page 165.
SAP R/3	Reportez-vous à la section "Clients SAP R/3" à la page .

Application ou famille de baies de disques	Référence
SAP MaxDB	Reportez-vous à la section "Clients SAP MaxDB" à la page 167.
Oracle Server	Reportez-vous à la section "Clients Oracle Server" à la page 167.
VMware	Reportez-vous à la section "Clients VMware" à la page 167.
IBM DB2 UDB	Reportez-vous à la section "Clients DB2" à la page 171.
HP Network Node Manager (NNM)	Reportez-vous à la section "Clients NNM" à la page 171.
Serveur NDMP (Network Data Management Protocol)	Reportez-vous à la section "Clients de serveur NDMP" à la page 171.
Service Microsoft Volume Shadow Copy (VSS)	Reportez-vous à la section "Clients Microsoft Volume Shadow Copy Service" à la page 172.
Lotus Notes/Domino Server	Reportez-vous à la section "Clients Lotus Notes/Domino Server" à la page 172.
EMC Symmetrix	Reportez-vous à la section "Intégration EMC Symmetrix" à la page 188.
HP StorageWorks P9000 XP Disk Array Family	Reportez-vous à la section "Intégration HP StorageWorks P9000 XP Disk Array Family" à la page 181.

Application ou famille de baies de disques	Référence
HP StorageWorks P6000 EVA Disk Array Family	Reportez-vous à la section "Intégration HP StorageWorks P6000 EVA Disk Array Family" à la page 173.

Tableau 6 Autres installations

Installation	Référence
Auto-migration avec Virtual Library System (VLS)	Reportez-vous à la section "Clients d'auto-migration VLS" à la page 195.
Interface utilisateur localisée	Reportez-vous à la section "Installation de l'interface utilisateur localisée de Data Protector" à la page 195.
Génération de rapports Web	Reportez-vous à la section "Installation des Rapports Web de Data Protector" à la page 201.
MC/ServiceGuard	Reportez-vous à la section "Installation de Data Protector sur MC/ServiceGuard" à la page 203.
Microsoft Cluster Server	Reportez-vous à la section "Installation de Data Protector sur Microsoft Cluster Server" à la page 204.
Veritas Cluster Server	Reportez-vous à la section "Installation de clients Data Protector sur un cluster Veritas" à la page 216.
Novell NetWare Cluster	Reportez-vous à la section "Installation de clients Data Protector sur un cluster Novell NetWare" à la page 217.
IBM HACMP Cluster	Reportez-vous à la section "Installation de Data Protector sur un cluster IBM HACMP" à la page 220.

Composants Data Protector

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

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

Interface utilisateur

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

REMARQUE :

Les commandes spécifiques de l'interface de ligne de commande Data Protector sont incluses dans d'autres composants Data Protector. Pour plus d'informations, reportez-vous au *Guide de référence de l'interface de ligne de commande HP Data Protector*.

Avant d'utiliser l'interface utilisateur de Data Protector dans des environnements hétérogènes, consultez les *Références, notes de publication et annonces produits HP Data Protector* pour prendre connaissance des limitations en vigueur.

Client d'interface Java

L'interface graphique Java de Data Protector est une interface utilisateur Java à architecture client-serveur. Elle contient l'interface utilisateur du Gestionnaire de cellule et l'interface utilisateur du MoM (Manager-of-Managers). Le client d'interface

	Java n'est pas sélectionné par défaut pour l'installation. Vous devez le sélectionner manuellement. Pour installer l'interface de ligne de commande sur un client disposant de l'interface utilisateur graphique Java, installez également le package Interface utilisateur ou un autre composant approprié de Data Protector sur ce système.
Documentation en anglais (guides, aide)	Il s'agit de la documentation et de l'aide en ligne en anglais de Data Protector.
Documentation en français (guides, aide)	Il s'agit de la documentation et de l'aide en ligne en français de Data Protector.
Documentation en japonais (guides, aide)	Il s'agit de la documentation et de l'aide en ligne en japonais de Data Protector.
Documentation en chinois simplifié (guides, aide)	Il s'agit de la documentation et de l'aide en ligne en chinois simplifié de Data Protector.
Interface utilisateur Manager-of-Managers	L'interface utilisateur du Manager-of-Managers (MoM) comprend l'interface utilisateur graphique de Data Protector. Ce logiciel est nécessaire pour accéder aux fonctionnalités Manager-of-Managers de Data Protector et pour contrôler l'environnement multicellules. L'interface utilisateur du Manager-of-Managers (MoM) et l'interface utilisateur Manager sont disponibles en tant qu'application commune.
Agent de disque	Le composant Agent de disque doit être installé sur les systèmes disposant de disques qui doivent être sauvegardés avec Data Protector.
Agent général de support	Le composant Agent général de support doit être installé sur les systèmes auxquels sont reliés des périphériques de sauvegarde ou qui disposent d'un accès au robot de bibliothèque et qui seront gérés avec Data Protector.

Auto-migration VLS	Le composant d'auto-migration de VLS doit être installé sur des clients qui réalisent des copies de supports intelligentes dans le système de bibliothèques virtuelles (VLS) en utilisant Data Protector.
Récupération après sinistre automatique	Le composant de récupération automatique après sinistre doit être installé sur les systèmes sur lesquels vous voulez 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.
Intégration SAP R/3	Le composant Intégration SAP R/3 doit être installé sur les systèmes 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 systèmes disposant d'une base de données SAP MaxDB qui sera sauvegardée avec Data Protector.
Intégration Oracle	Le composant Intégration Oracle doit être installé sur les systèmes disposant d'une base de données Oracle qui sera sauvegardée avec Data Protector.
Intégration VMware (hérité)	Le composant Intégration VMware (hérité) doit être installé sur les systèmes VirtualCenter (s'ils existent) et sur tous les systèmes ESX Server que vous envisagez de sauvegarder avec Data Protector. Si vous envisagez d'utiliser la méthode de sauvegarde VCBfile ou VCBimage, le composant d'intégration doit également être installé sur les systèmes de sauvegarde proxy.
Intégration de l'environnement virtuel	Le composant Intégration de l'environnement virtuel doit être installé sur les systèmes que vous allez utiliser en tant qu'hôtes de sauvegarde pour

	gérer la sauvegarde et la restauration des machines virtuelles à l'aide du composant Data Protector Intégration de l'environnement virtuel. Pour la sauvegarde et la restauration de systèmes Microsoft Hyper-V, le composant d'intégration doit également être installé sur tous les systèmes Microsoft Hyper-V à sauvegarder, avec le composant Intégration MS Volume Shadow Copy.
Intégration DB2	Le composant Intégration DB2 doit être installé sur tous les systèmes disposant d'un serveur DB2 qui sera sauvegardé avec Data Protector.
Intégration Sybase	Le composant Intégration Sybase doit être installé sur les systèmes disposant d'une base de données Sybase qui sera sauvegardée avec Data Protector.
Intégration Informix	Le composant Intégration Informix doit être installé sur les systèmes disposant d'une base de données Informix Server qui sera sauvegardée avec Data Protector.
Intégration de MS Exchange	Le composant Intégration MS Exchange doit être installé sur les systèmes Microsoft Exchange Server 2003/2007 que vous prévoyez de sauvegarder via l'intégration de Data Protector avec Microsoft Exchange Server 2003/2007 ou l'intégration de Data Protector avec la boîte aux lettres Microsoft Exchange unique. Il doit également être installé sur les systèmes Microsoft Exchange Server 2010 que vous prévoyez de sauvegarder via l'intégration de Data Protector avec la boîte aux lettres Microsoft Exchange unique.
Intégration MS Exchange Server 2010	Le composant Intégration MS Exchange Server doit être installé sur les systèmes Microsoft Exchange Server 2010 que vous prévoyez de sauvegarder via l'intégration de Data Protector avec Microsoft Exchange Server 2010.

Intégration MS SQL	Le composant Intégration SQL doit être installé sur les systèmes où une base de données Microsoft SQL Server sera sauvegardée avec Data Protector.
Intégration MS SharePoint Portal Server	Le composant Intégration MS SharePoint Portal Server doit être installé sur les systèmes Microsoft SharePoint Portal Server qui seront sauvegardés avec Data Protector.
Intégration MS SharePoint 2007/2010	Le composant Intégration MS SharePoint 2007/2010 doit être installé sur les systèmes Microsoft SharePoint Server 2007/2010 qui seront sauvegardés avec Data Protector.
Intégration du service MS Volume Shadow Copy	Le composant Intégration du service MS Volume Shadow Copy doit être installé sur les systèmes Windows Server sur lesquels vous souhaitez exécuter des sauvegardes coordonnées par le service Volume Shadow Copy.
Agent HP StorageWorks P6000 EVA SMI-S	Le composant Agent HP StorageWorks P6000 EVA SMI-S doit être installé sur le système d'application et de sauvegarde pour intégrer HP StorageWorks P6000 EVA Disk Array Family dans Data Protector.
Agent HP StorageWorks P9000 XP	Le composant Agent HP StorageWorks P9000 XP doit être installé sur les systèmes d'application et de sauvegarde pour intégrer HP StorageWorks P9000 XP Disk Array Family dans Data Protector.
Agent HP StorageWorks P4000	Le composant Agent HP StorageWorks P4000 doit être installé sur les systèmes d'application et de sauvegarde pour intégrer HP StorageWorks P4000 SAN Solutions dans Data Protector.
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.

Intégration HP Network Node Manager	Le composant Intégration NNM doit être installé sur tous les systèmes de la cellule où réside la base de données NNM devant être sauvegardée avec Data Protector.
Agent de support NDMP	L'Agent de support NDMP doit être installé sur tous les systèmes qui sauvegardent des données vers des lecteurs dédiés NDMP via un serveur NDMP.
Intégration Lotus	Le composant Intégration Lotus doit être installé sur tous les systèmes de la cellule Data Protector où réside une base de données Lotus Notes/Domino Server qui sera sauvegardée avec Data Protector.
Extension de restauration granulaire MS SharePoint	L'extension de restauration granulaire Data Protector pour Microsoft SharePoint Server doit être installée sur le système Administration centrale de Microsoft SharePoint Server.
Plug-in Web de l'extension de restauration granulaire VMware	Le composant Data Protector Plug-in Web de l'extension de restauration granulaire VMware doit être installé sur le serveur virtuel VMware afin d'activer la fonction de restauration granulaire pour les machines virtuelles VMware. Seule l'installation à distance est prise en charge.
Agent de l'extension de restauration granulaire VMware	Le composant Data Protector Agent de l'extension de restauration granulaire VMware doit être installé sur le système proxy de montage afin d'activer les fonctions de restauration standard et de restauration granulaire pour les machines virtuelles VMware. Seule l'installation à distance est prise en charge.

REMARQUE :

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

Installation distante de clients Data Protector

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

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.

Configuration système requise

- Pour connaître les conditions préalables et les recommandations d'installation, reportez-vous à la section décrivant la procédure d'installation pour ce client particulier. Les références sont énumérées dans le Tableau 4 à la page 73 et le Tableau 5 à la page 74.
- Rendez-vous sur http://www.hp.com/support/manuals et reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector* pour plus d'informations sur les plates-formes et composants Data Protector pris en charge, ainsi que sur l'espace disque nécessaire.
- A ce stade de la procédure, le Gestionnaire de cellule et le(s) Serveur(s) d'installation doivent être installés sur votre réseau.
- Le Serveur d'installation pour Windows doit résider dans un répertoire partagé pour être visible dans l'ensemble du réseau.

Recommandations

- ***Systèmes UNIX :*** pour des raisons de sécurité, il est recommandé d'utiliser un shell sécurisé pour l'installation à distance de Data Protector. En l'absence de shell sécurisé, les outils UNIX hérités `rsh` et `rexec` sont automatiquement utilisés par le programme d'installation à distance de Data Protector.

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

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 utilisateur graphique connectée à chaque Gestionnaire de cellule à tour de rôle.

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 systèmes UNIX seulement.

Configuration de OpenSSH

Installez et configurez OpenSSH sur le client et le Serveur d'installation :

1. Vérifiez que OpenSSH est installé sur votre système. Pour plus d'informations, reportez-vous à la documentation de votre système d'exploitation ou distribution.

   Si le package OpenSSH n'est pas inclus dans votre distribution de système d'exploitation, téléchargez-le à partir du site http://www.openssh.org, puis installez-le sur le client Data Protector et le Serveur d'installation.

   Sous HP-UX, vous pouvez également utiliser HP-UX Secure Shell.

   REMARQUE :

   L'emplacement par défaut de l'installation via un shell sécurisé est le suivant : `/opt/ssh`.

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

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

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

REMARQUE :

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

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

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

   `répertoire_installation_ssh/ssh/etc/ssh_config`

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

2. ***Sur le client :***

   `répertoire_installation_ssh/ssh/etc/sshd_config`

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

Notez que ces deux fichiers doivent être synchronisés.

REMARQUE :

La version de protocole SSH par défaut est SSH2.

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

   `répertoire_installation_ssh/ssh/sbin/sshd`

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

   `ssh root@hôte_client`

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

   `ssh root@client1.société.com`

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

Configuration de Keychain

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

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

   HP-UX, Solaris :

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

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

   Linux :

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

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

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

Etape suivante

Après avoir configuré OpenSSH et Keychain, ajoutez des clients à la cellule à l'aide de l'interface graphique, comme décrit à la section Ajout de clients à la cellule à la page 87, ou à l'aide de l'interface de ligne de commande en exécutant la commande `ob2install`. Pour plus d'informations sur les commandes de l'interface de ligne de commande et leurs paramètres, reportez-vous au *Guide de référence de l'interface de ligne de commande HP Data Protector*.

REMARQUE :

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

Ajout de clients à la cellule

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 utilisateur graphique de Data Protector :
   - Interface graphique d'origine de Data Protector (sous Windows uniquement) :
     - **Démarrer** > **Programmes** > **HP Data Protector** > **Gestionnaire Data Protector**.
   - Interface utilisateur graphique Java de Data Protector :
     - Sous Windows : Sélectionnez **Démarrer** > **Programmes** > **HP Data Protector** > **Gestionnaire de l'interface Java Data Protector**.

       Dans la boîte de dialogue Se connecter à un Gestionnaire de cellule, sélectionnez ou entrer le nom d'un Gestionnaire de cellule et cliquez sur `Connexion`.
     - Sous UNIX, exécutez :

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

   Reportez-vous à la section “Interface utilisateur graphique de Data Protector” à la page 40 et à l'aide en ligne pour plus de détails sur l'interface utilisateur graphique de Data Protector.
2. Dans le Gestionnaire Data Protector, sélectionnez le contexte **Clients**.
3. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Clients**, puis cliquez sur **Ajouter clients**.
4. Si plusieurs Serveurs d'installation sont configurés, sélectionnez la plate-forme des clients à installer (UNIX ou Windows) et le Serveur d'installation à utiliser pour la procédure. Cliquez sur **Suivant**.

5. Entrez les noms des clients ou recherchez les clients (interface Windows uniquement) à installer comme l'illustre la Figure 14 à la page 88. Cliquez sur **Suivant**.

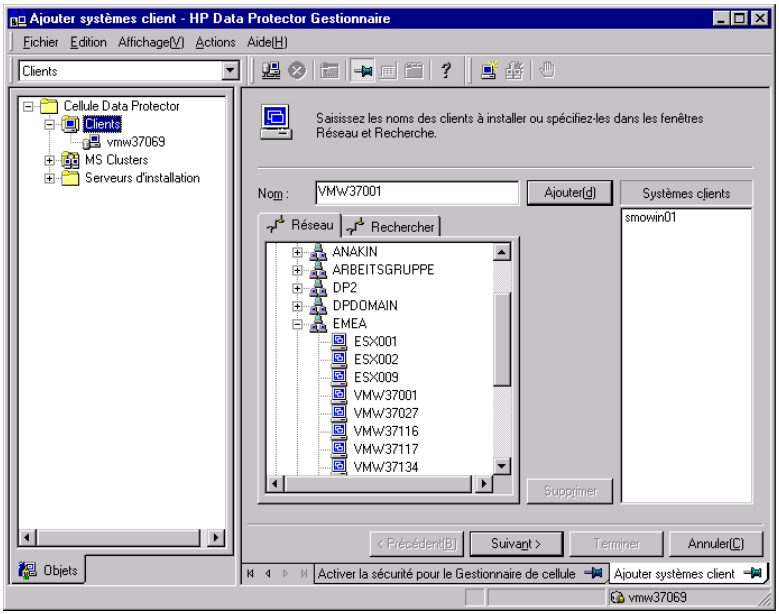


Figure 14 Sélection de clients

6. Sélectionnez les composants Data Protector à installer comme l'illustre la Figure 15 à la page 89. Notez que vous ne pouvez sélectionner qu'un type d'Agent de support. Reportez-vous à la section “Composants Data Protector” à la page 77.

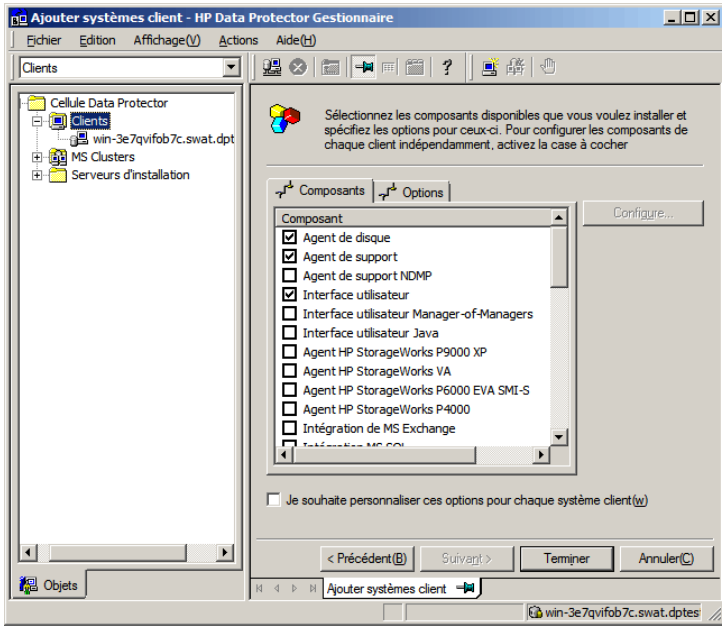


Figure 15 Sélection de composants

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

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

Cliquez sur **Terminer** pour démarrer l'installation.

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

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

REMARQUE :

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

Dépannage

Dès que l'installation à distance est terminée, vous pouvez relancer les procédures d'installation qui ont échoué via l'interface en cliquant sur **Actions** et **Redémarrer clients ayant échoué**. Si l'installation échoue de nouveau, reportez-vous au Chapitre 6 à la page 367.

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 268.

Clients MC/ServiceGuard

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

Condition préalable

Le Serveur d'installation correspondant doit être disponible.

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

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

4. Sélectionnez les clients sur lesquels vous souhaitez installer les composants comme illustré dans la Figure 16 à la page 91. Cliquez sur **Suivant**.

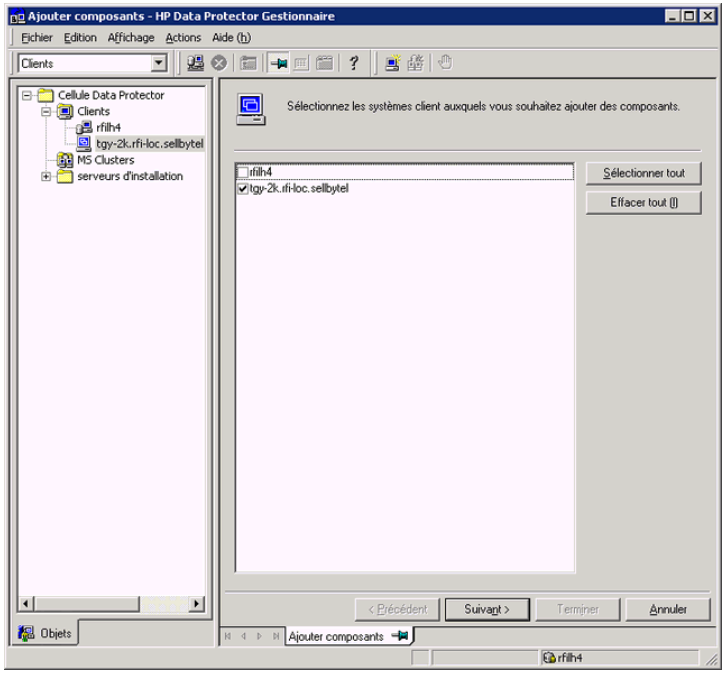


Figure 16 Sélection de clients

5. Sélectionnez les composants Data Protector à installer comme l'illustre la Figure 17 à la page 92. Notez que vous ne pouvez sélectionner qu'un type d'Agent de support. Reportez-vous à la section “Composants Data Protector” à la page 77.

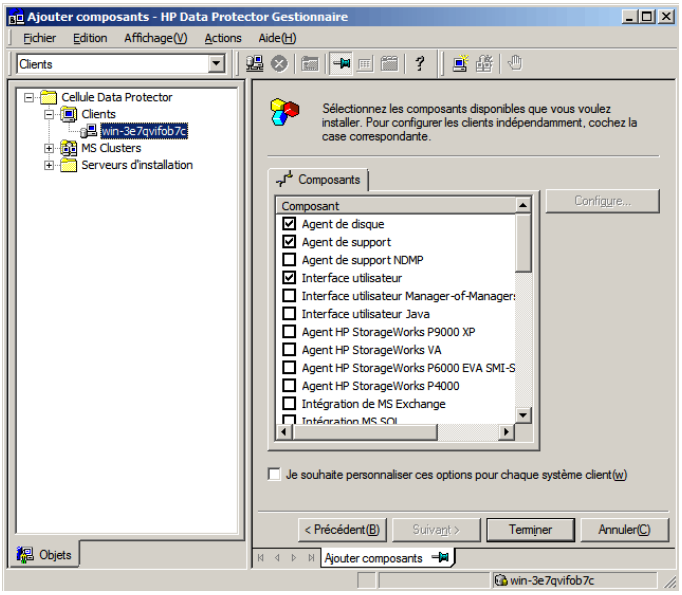


Figure 17 Sélection de composants

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

Cliquez sur **Terminer** pour démarrer l'installation.

Installation de clients Windows

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

Configuration système requise

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

- Disposer de Microsoft Internet Explorer 5.0 ou supérieur.
- Disposer d'un espace disque suffisant pour le logiciel client Data Protector. Pour plus d'informations à ce sujet, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Disposer du port numéro 5555 (par défaut).
- Disposer de l'implémentation Microsoft du protocole TCP/IP, lequel doit être installé et en cours d'exécution. Ce protocole doit pouvoir résoudre les noms d'hôte. Les noms de l'ordinateur et de l'hôte doivent être identiques.
- Pour le client d'interface Java, une version prise en charge de l'environnement JRE (Java Runtime Environment) est nécessaire. Reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector* ou aux dernières matrices de support à l'adresse http://www.hp.com/support/manuals.
- Vérifiez que les droits d'accès au réseau sont définis sous la règle de sécurité locale Windows pour le compte qui procède à l'installation.

Limites

- En raison des restrictions de sécurité imposées par le système d'exploitation Windows, le Serveur d'installation peut être utilisé pour installer des clients à distance uniquement dans le même domaine.
- Sous Windows XP Edition familiale, les clients Data Protector peuvent uniquement être installés en local.
- Lors de l'installation à distance de clients sur des systèmes Windows Vista, Windows 7 et Windows Server 2008, vous devez utiliser l'un des comptes suivants :
  - Un compte administrateur intégré sur le système distant. Le compte doit être activé et le *mode approbation d'administrateur* désactivé.
  - Un compte utilisateur de domaine, qui est membre d'un groupe Administrateurs local sur le système distant.

Recommandation

Sur chaque client Windows, assurez-vous que vous disposez de Microsoft Installer (MSI) 2.0 avant d'installer Data Protector 6.20. Si vous possédez une version plus ancienne de MSI, le programme d'installation de Data Protector va automatiquement le mettre à niveau avec la version 2.0. Dans ce cas, Data Protector affichera une remarque à la fin de l'installation, indiquant que MSI a été mis à niveau. Si MSI a été mis à niveau, il est vivement recommandé de redémarrer le système client. Consultez le support technique Microsoft pour connaître la configuration requise pour Microsoft Installer 2.0 sur les différents systèmes d'exploitation Windows.

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

Récupération après sinistre automatique

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

Clients compatibles cluster

D'autres conditions sont requises pour l'installation de clients compatibles cluster. Pour plus de détails, reportez-vous à la section "Installation de clients compatibles cluster" à la page 213.

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 77.

Installation locale

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

1. Insérez le DVD-ROM.

   Sur les systèmes Windows Vista, Windows 7 et Windows Server 2008, la boîte de dialogue Contrôle du compte utilisateur s'affiche. Cliquez sur **Continuer** pour poursuivre l'installation.

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

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

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

5. Saisissez le nom du Gestionnaire de cellule. Reportez-vous à la Figure 18 à la page 95.

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

   Cliquez sur **Suivant**.

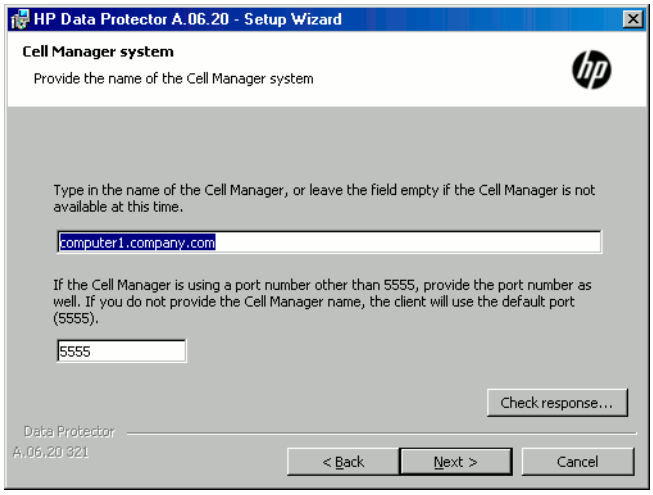


Figure 18 Choix du Gestionnaire de cellule

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

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

7. Sélectionnez les composants de Data Protector à installer.

   Pour obtenir des informations sur les composants Data Protector, reportez-vous à la section “Composants Data Protector” à la page 77.

   Cliquez sur **Suivant**.

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

   Cliquez sur **Suivant**.

9. La liste des composants sélectionnés s'affiche. Cliquez sur **Installer** pour démarrer l'installation des composants sélectionnés.

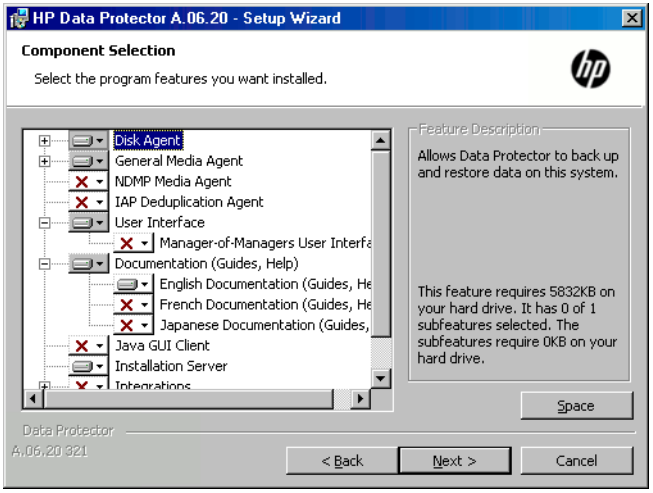


Figure 19 Page de résumé des composants sélectionnés

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

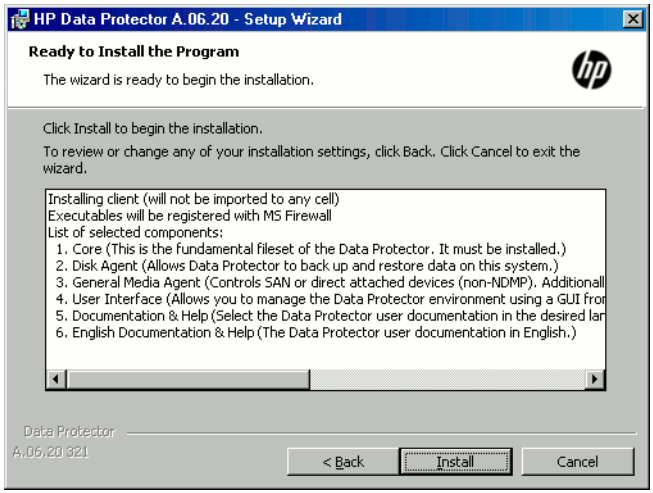


Figure 20 Page de résumé de l'installation

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

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

    Cliquez sur **Terminer**.

Connexion d'un périphérique de sauvegarde aux systèmes Windows

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

1. Recherchez les adresses SCSI disponibles (désignées sous le nom de *ID SCSI cibles* sous Windows) pour les lecteurs et le périphérique de contrôle (robot) du périphérique de sauvegarde à connecter. Reportez-vous à la section "Recherche des ID SCSI cibles inutilisés sur un système Windows" à la page 446.
2. Définissez les `ID SCSI cibles` inutilisés pour les lecteurs et le périphérique de contrôle (robot). En fonction du type de périphérique, vous pouvez généralement effectuer cette opération avec les commutateurs du périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

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

3. Eteignez votre ordinateur et connectez le périphérique de sauvegarde au système.
4. Allumez le périphérique, puis l'ordinateur, et attendez que le processus d'amorçage soit terminé.
5. Pour vérifier que le système reconnaît correctement votre nouveau périphérique de sauvegarde, dans le répertoire `répertoire_Data_Protector\bin`, exécutez la commande `devbra -dev`.

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

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

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

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

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

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

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

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

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

Pour charger ou décharger le pilote de bandes d'origine de votre périphérique, reportez-vous à la section “Utilisation de pilotes de bandes et de pilotes de robots sous Windows” à la page 425. 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 429.

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 HP-UX ou Solaris et Linux, 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 77.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes, processeurs et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Le cas échéant, reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector” à la page 44 pour obtenir des instructions.
- Vous devez disposer soit d'un accès *root*, soit d'un compte doté des droits *root*.
- Pour le client d'interface Java, une version prise en charge de l'environnement JRE (Java Runtime Environment) est nécessaire. Reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector* ou aux dernières matrices de support à l'adresse http://www.hp.com/support/manuals.

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 HP-UX ou Solaris et Linux. Reportez-vous à la section “Installation en local de clients UNIX et Mac OS X” à la page 151 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 222.

Installation distante

Vous devez installer le logiciel client à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface utilisateur graphique 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 83.

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 de clients compatibles cluster” à la page 204.

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 431.

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

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

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

   - Les pilotes des périphériques que vous allez utiliser doivent apparaître dans la liste des pilotes installés. Reportez-vous à la Figure 21 à la page 101. Si le pilote que vous recherchez n'est pas mentionné, vous devez l'installer à l'aide de l'utilitaire `/usr/sbin/swinstall`. Par exemple :
     - Un pilote de périphériques à bandes est requis pour les périphériques à bande et doit être installé si vous souhaitez connecter ce type de périphérique au système. Par exemple, le pilote `stape` est utilisé pour les lecteurs de bande SCSI génériques de type DLT ou LTO, alors que le pilote `tape2` est réservé aux périphériques DDS.
     - Un pilote de passage SCSI nommé `sctl` ou `spt`, ou un pilote de robot de changeur automatique nommé `schgr` (selon le matériel) est requis pour contrôler le robot des périphériques de bibliothèque de bande.

       Pour plus de détails, reportez-vous à la section "Configuration de robot SCSI sous HP-UX" à la page 431.

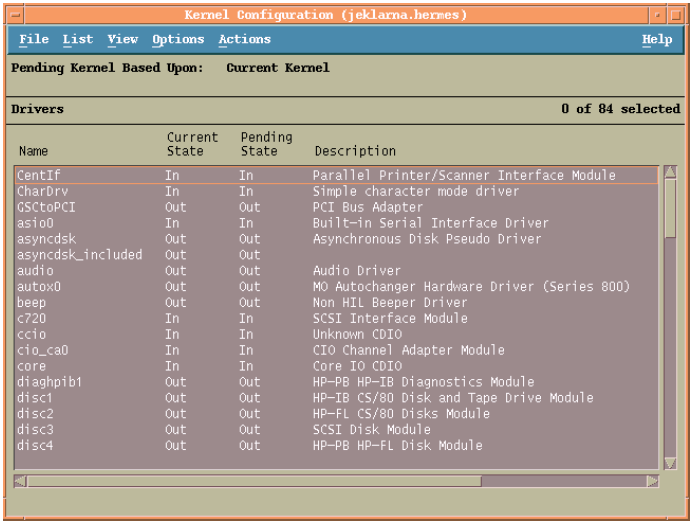


Figure 21 Fenêtre de configuration du kernel

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

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

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

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

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

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

   Pour plus d'informations, reportez-vous à la section "Recherche des adresses SCSI non utilisées sous HP-UX" à la page 438.

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

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

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

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

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

   de manière à pouvoir visualiser la liste des fichiers de chaque périphérique de sauvegarde connecté. Si un fichier de périphérique n'a pas été créé automatiquement durant le processus d'amorçage, vous devez le créer manuellement. Reportez-vous à la section "Création de fichiers de périphérique sous HP-UX" à la page 435.

Lorsque vous avez terminé l'installation et connecté correctement les périphériques de sauvegarde au système, recherchez l'entrée suivante dans l'index de l'aide en ligne : "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 HP-UX, ou Solaris et Linux 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 77.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 44 pour obtenir des instructions.
- Pour installer un client Solaris, vous devez disposer soit d'un accès *root*, soit d'un compte doté des droits *root*.
- Pour le client d'interface Java, une version prise en charge de l'environnement JRE (Java Runtime Environment) est nécessaire. Reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector* ou aux dernières matrices de support à l'adresse http://www.hp.com/support/manuals.

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 HP-UX, ou Solaris et Linux. Reportez-vous à la section "Installation en local de clients UNIX et Mac OS X" à la page 151 pour obtenir des instructions.

Installation distante

Vous devez installer le logiciel client à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface utilisateur graphique 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 83.

REMARQUE :

Si vous installez le composant `Interface utilisateur` (comprenant l'interface utilisateur graphique 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 54.

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 de clients compatibles cluster" à la page 216.

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

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

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

REMARQUE :

La bibliothèque HP StorageWorks 12000e ne possède pas d'ID SCSI dédié pour le périphérique sélectionneur, mais les commandes d'accès au lecteur de données et les commandes sélectionneur sont acceptées pour le même ID SCSI. Les commandes d'accès au lecteur de données doivent toutefois être dirigées vers SCSI lun=0 et les commandes sélectionneur vers 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 plus d'information sur les périphériques pris en charge, reportez-vous au site http://www.hp.com/support/manuals.

   REMARQUE :

   Data Protector ne reconnaît pas automatiquement les bandes nettoyantes sur un système Solaris. Si Data Protector détecte et insère une bande nettoyante dans le périphérique HP StorageWorks 12000e (48AL), le pilote de bandes prend un état non défini et peut exiger le réamorçage du 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/0hb` (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 systèmes clients Linux peuvent être installés en local à partir du DVD-ROM d'installation HP-UX, ou Solaris et Linux 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 77.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector” à la page 44 pour de plus amples informations.
- L'utilitaire `rpm` doit être installé et configuré. Les autres systèmes de gestion de packages (tels que `deb`) ne sont pas pris en charge.
- Pour le client d'interface Java, une version prise en charge de l'environnement JRE (Java Runtime Environment) est nécessaire. Reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector* ou aux dernières matrices de support à l'adresse http://www.hp.com/support/manuals.
- L'installation des composants Data Protector sur un *système distant* est soumise aux conditions préalables suivantes sur le système distant :
  - Le service `inetd` ou `xinetd` doit être actif ou configuré pour que Data Protector puisse le démarrer.
  - Le service `ssh` ou, si `ssh` n'est pas installé, le service `rexec` doit être activé.
- Vérifiez que le noyau prend en charge les périphériques SCSI (modules `Prise en charge SCSI`, `Prise en charge de bandes SCSI` et `Prise en charge générique SCSI`). Le paramètre `Explorer tous les LUNS de chaque périphérique SCSI` est facultatif.

  Reportez-vous à la documentation de votre distribution Linux ou à la documentation du noyau Linux pour plus d'informations sur la prise en charge SCSI dans le noyau Linux.

REMARQUE :

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

REMARQUE :

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

Si ce numéro de port est déjà utilisé, vous devez le rendre disponible pour Data Protector ou remplacer cette valeur par défaut par le numéro d'un port non utilisé. Reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 414.

Cluster MC/ServiceGuard

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

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

Vous pouvez utiliser le nœud passif pour installer un Serveur d'installation.

Novell Open Enterprise Server (OES)

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

- Si vous installez Novell OES sur un serveur SUSE Linux Enterprise Server 9.0 (SLES) 32 bits après avoir installé un client Linux Data Protector sur un système, vous devez également mettre à niveau le client Data Protector.

  Notez que le nouvel agent de disque compatible Novell OES sera installé à distance sur le système client au cours de cette mise à niveau.

- Si vous supprimez le composant Novell OES du SLES, vous devez réinstaller le client Data Protector.

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour HP-UX, ou Solaris et Linux. Reportez-vous à la section "Installation en local de clients UNIX et Mac OS X" à la page 151 pour de plus amples informations.

Installation distante

Vous pouvez installer à distance un système client Linux en distribuant les composants Data Protector à partir du Serveur d'installation pour UNIX sur le système Linux, à l'aide de l'interface utilisateur graphique 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 83.

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

Résolution des problèmes d'installation à distance

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

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

   ```
   server_args = -h
   ```

   Par exemple :

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

   REMARQUE :

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

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

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

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

Après avoir installé Data Protector, vous pouvez supprimer l'entrée du fichier `-root/.rhosts`, l'indicateur `-h` du fichier `/etc/xinetd.conf` (`/etc/inetd.conf` pour Red Hat Enterprise Linux). Répétez ensuite la commande `kill` décrite à l'Étape 2 à la page 114.

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 en local de clients UNIX et Mac OS X” à la page 151.

Connexion d'un périphérique de sauvegarde à un système Linux

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

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

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

Exemples

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

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

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

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

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

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

   Par exemple :

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

   Le résultat de cette commande est le suivant :

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

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

Etape suivante

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

Installation des clients ESX Server

ESX Server est un système d'exploitation Linux modifié. Pour plus d'informations sur l'installation des composants Data Protector sur des systèmes ESX Server, reportez-vous à la section “Installation de clients Linux” à la page 110.

Installation des clients Mac OS X

Les clients Mac OS X peuvent être installés en local à partir du DVD-ROM d'installation HP-UX, ou Solaris et Linux ou à distance à l'aide du Serveur d'installation pour UNIX.

Seul l'Agent de disque (AD) est pris en charge.

Conditions préalables

- Pour connaître la configuration système requise, l'espace disque requis, et les versions de système d'exploitation et composants Data Protector pris en charge,

reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector*.

- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Pour obtenir des instructions, reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 44.

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 HP-UX, ou Solaris et Linux. Pour obtenir des instructions, reportez-vous à la section "Installation en local de clients UNIX et Mac OS X" à la page 151.

Installation distante

Vous devez installer le logiciel client Mac OS X à partir du Serveur d'installation pour UNIX sur les clients via l'interface utilisateur graphique de Data Protector. Pour connaître la procédure détaillée d'installation du logiciel à distance, reportez-vous à la section "Installation distante de clients Data Protector" à la page 83.

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

Installation de clients AIX

Les clients AIX peuvent être installés en local à partir du DVD-ROM d'installation HP-UX, ou Solaris et Linux 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 77.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 44 pour obtenir des instructions.

IMPORTANT :

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

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

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

Cluster IBM HACMP

Dans l'environnement IBM HACMP (High Availability Cluster Multi-Processing) pour AIX, installez le composant `Agent de disque` Data Protector sur tous les noeuds du cluster. Pour plus d'informations sur l'installation de Data Protector dans un environnement de cluster comprenant une application de base de données compatible cluster, reportez-vous à la section "Installation des clients d'intégration Data Protector" à la page 157.

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

Installation en local

Si aucun Serveur d'installation pour UNIX n'est installé dans votre environnement, vous devez procéder à une installation en local à partir du DVD-ROM d'installation pour HP-UX, ou Solaris et Linux. Reportez-vous à la section "Installation en local de clients UNIX et Mac OS X" à la page 151 pour obtenir des instructions.

Installation distante

Vous devez installer le logiciel client AIX à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface utilisateur graphique 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 83.

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

Connexion d'un périphérique de sauvegarde à un client AIX

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

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

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

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

IMPORTANT :

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

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

IMPORTANT :

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

Etape suivante

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

Installation de clients Tru64

Les clients Tru64 peuvent être installés en local à partir du DVD-ROM d'installation HP-UX, ou Solaris et Linux 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 77.

Conditions préalables

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector à la page 44 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 HP-UX, ou Solaris et Linux. Reportez-vous à la section "Installation en local de clients UNIX et Mac OS X à la page 151 pour de plus amples informations.

Installation distante

Vous devez installer le logiciel client Tru64 à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface utilisateur graphique 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 83.

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

Cluster Tru64

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

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

Après l'installation, il faut importer le nom d'hôte virtuel du cluster et les différents nœuds dans la cellule Data Protector. Pour connaître la procédure, reportez-vous à la section “Importation d'un client compatible cluster dans une cellule” à la page 225

Connexion d'un périphérique de sauvegarde à un client Tru64

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

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

   REMARQUE :

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

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

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

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

Etape suivante

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

Installation de clients SCO

Les clients SCO peuvent être installés en local à partir du DVD-ROM d'installation HP-UX, ou Solaris et Linux 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 77.

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- A ce stade de la procédure, le Gestionnaire de cellule et le Serveur d'installation pour UNIX doivent être installés sur votre réseau. Reportez-vous à la section "Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector" à la page 44 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 HP-UX, ou Solaris et Linux. Reportez-vous à la section "Installation en local de clients UNIX et Mac OS X" à la page 151 pour de plus amples informations.

Installation distante

Vous devez installer le logiciel client SCO à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface utilisateur graphique 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 83.

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

Connexion d'un périphérique de sauvegarde à un système SCO

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

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

   Pour plus d'information sur les périphériques pris en charge, reportez-vous au site http://www.hp.com/support/manuals et à la documentation fournie avec chaque périphérique.
2. Eteignez votre ordinateur et connectez le périphérique de sauvegarde au bus SCSI.
3. Redémarrez votre ordinateur.

4. Configurez le périphérique à l'aide de la commande `mkdev tape`. Dans la liste des types de lecteurs de bande, sélectionnez le `lecteur de bande SCSI-1 / SCSI-2 générique`.

REMARQUE :

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

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

   Utilisez le nom `nrStp#`, dans lequel # représente l'ID D'UNITE du périphérique. L'ID D'UNITE du périphérique est définie à l'Étape 4 à la page 123. Le nom de fichier de périphérique `/dev/nrStp#` est expliqué à la Figure 22 à la page 124.

△ ATTENTION :

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

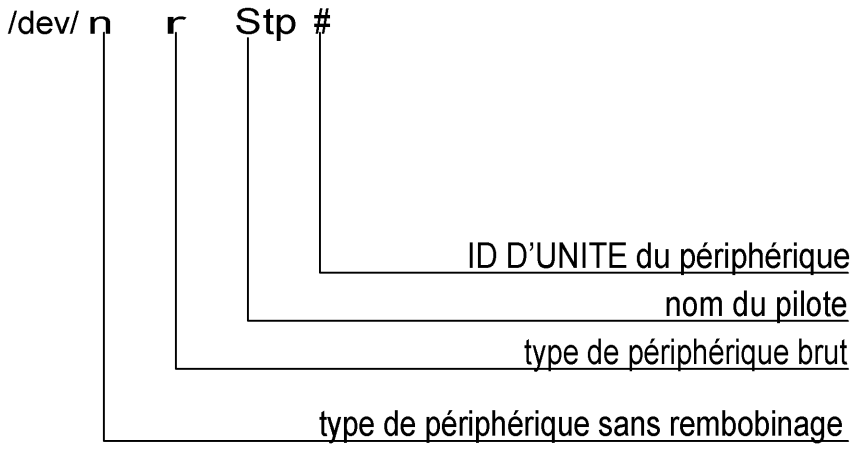


Figure 22 Format de nom de fichier de périphérique

Etape suivante

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

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

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

Pour la bibliothèque ADIC/GRAU, chaque système sur lequel vous installez un Agent de support et qui accède au robot de bibliothèque via le serveur DAS GRAU/ADIC est appelé **client 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 à la page 327.

Connexion de lecteurs de bibliothèque

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

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

Reportez-vous à la section "Installation de clients HP-UX" à la page 99 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 92 pour savoir comment connecter physiquement un périphérique de sauvegarde à un système Windows pris en charge. Consultez également la documentation fournie avec la bibliothèque ADIC/GRAU ou StorageTek.

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

La procédure suivante concerne la configuration d'une bibliothèque ADIC/GRAU.

Vous devez suivre cette procédure avant d'installer le logiciel Agent de support :

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

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

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

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

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

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

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

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

   ```
   OB2_ACIEJECTTOTAL = 0
   ```

REMARQUE :

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

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

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

Configuration système requise

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

- La bibliothèque ADIC/GRAU doit être configurée et fonctionner. Consultez la documentation fournie avec la bibliothèque ADIC/GRAU pour en savoir plus à ce sujet.
- Data Protector doit être installé et configuré. Pour connaître la procédure à suivre, reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector” à la page 44 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 102.

- 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 97.

Installation

La procédure d'installation est la suivante :

1. Distribuez le composant Agent de support aux clients à l'aide de l'interface utilisateur graphique 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 83 de ce chapitre.

2. Installez la bibliothèque ADIC/GRAU :

   - Avec un système Windows, procédez comme suit :
     a. Copiez les bibliothèques `aci.dll`, `winrpc32.dll` et `ezrpc32.dll` dans le répertoire `répertoire_Data_Protector\bin`. (Ces trois bibliothèques font partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU ; vous pouvez les trouver sur le support d'installation ou dans le répertoire `C:\DAS\AMU\` de l'AMU-PC).
     b. Copiez également ces trois fichiers dans le répertoire `%SystemRoot%\system32`.
     c. Copiez `Portinst` et le `service Portmapper` dans le client DAS (ces éléments font partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU ; vous les trouverez sur le support d'installation).
     d. Dans le Panneau de configuration, ouvrez `Outils d'administration, Services` et lancez `portinst` pour installer `portmapper`. Vous devez relancer le client DAS pour exécuter le service `portmapper`.
     e. Après avoir réamorcé le système, vérifiez que `portmapper` et les deux `services rpc` sont exécutés (dans le Panneau de configuration, ouvrez **Outils d'administration, Services** et vérifiez l'état des services).
   - Sur un système HP-UX, copiez la bibliothèque partagée `libaci.sl` dans le répertoire `/opt/omni/lib`. Vous devez avoir les autorisations nécessaires pour accéder à ce répertoire. Vérifiez que la bibliothèque partagée dispose bien des autorisations de lecture et d'exécution pour tout le monde (root, groupe et autre). La bibliothèque partagée `libaci.sl` fait partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU ; vous la trouverez sur le support d'installation.
   - Sur un système AIX, copiez la bibliothèque partagée `libaci.sl` dans le répertoire `/usr/omni/lib`. Vous devez avoir les autorisations nécessaires pour accéder à ce répertoire. Vérifiez que la bibliothèque partagée dispose bien des autorisations de lecture et d'exécution pour tout le monde (root, groupe et autre). La bibliothèque partagée `libaci.o` fait partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU ; vous la trouverez sur le support d'installation.

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

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

Systèmes Windows : `répertoire_Data_Protector\bin\devbra -dev`

Systèmes HP-UX : `/opt/omni/lbin/devbra -dev`

Systèmes 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 44.
- 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&gt; 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 102.

- 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 97.

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

  Si un CAP n'est pas dans l'état `en ligne`, changez l'état avec la commande suivante : `vary cap id_cap online`

  Si un CAP n'est pas en mode de fonctionnement `manuel`, changez le mode avec la commande suivante : `set cap manual id_cap`

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

La procédure d'installation est la suivante :

1. Distribuez le composant Agent de support aux clients à l'aide de l'interface utilisateur graphique 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 83 de ce chapitre.
2. Exécutez le démon ACS `ssi` pour chaque client ACS :
   - Sur des clients HP-UX, Solaris et Linux, exécutez la commande suivante :
     `/opt/omni/acs/ssi.sh start nom_hôte_LS_ACS`
   - Sur des clients ACS Windows, installez le service `LibAttach`. Pour plus de détails à ce sujet, reportez-vous à la documentation ACS. Vérifiez que le nom d'hôte d'ACSLS approprié est entré pendant la configuration du service `LibAttach`. Au terme d'une configuration réussie, les services `LibAttach` sont lancés automatiquement. Ils seront également lancés automatiquement après chaque réamorçage.
   - Sur des clients ACS AIX, exécutez la commande suivante :
     `/usr/omni/acs/ssi.sh start nom_hôte_LS_ACS`

REMARQUE :

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

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

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

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

Etape suivante

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

Installation en local de clients Novell NetWare

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

Vous pouvez installer l'Agent de disque et l'Agent général de support Data Protector sur les systèmes exécutant Novell NetWare. Pour obtenir des informations sur les composants Data Protector, reportez-vous à la section “Composants Data Protector” à la page 77.

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

Configuration système requise

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

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

    Ce service doit s'exécuter sur Windows lorsqu'une installation est exécutée à partir du serveur Windows.
  - Client Novell pour Windows ou service client Microsoft pour NetWare.

    Ce service doit s'exécuter sur Windows lorsqu'une installation est exécutée à partir de la station de travail Windows.
- Connectez-vous au serveur NetWare cible (ou à l'arborescence NDS/eDirectory appropriée) à partir du système Windows.

- Vérifiez que vous disposez bien des droits de superviseur pour le volume SYS: sur le serveur NetWare cible.
- Assurez-vous qu'au moins un nom de périphérique local est libre sur le système Windows.

Clients compatibles cluster

D'autres conditions sont requises pour l'installation de clients compatibles cluster. Pour plus de détails, reportez-vous à la section “Installation de clients compatibles cluster” à la page 218.

Installation

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

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

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

2. Exécutez le script d'installation.

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

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

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

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

REMARQUE :

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

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

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

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

UNLOAD HPINET (UNLOAD OMNIINET / UNLOAD HPBRAND)

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

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

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

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

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

   SEARCH ADD SYS:USR\OMNI\BIN

   LOAD HPINET.NLM

REMARQUE :

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

LOAD HPINET.NLM -port *numéro_port*

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

REMARQUE :

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

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

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

   ```
   LOAD HPLOGIN.NLM
   ```

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

   - Contexte NDS/eDirectory :

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

     `OU=SDM.O=MONDOMAINE`

   - 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=MONDOMAINE`.

   - Mot de passe d'objet NDS/eDirectory :

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

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

REMARQUE :

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

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

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

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

REMARQUE :

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

CONSEIL :

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

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

Configuration de l'Agent de support

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

Data Protector prend en charge l'adaptateur hôte SCSI Adaptec et le pilote .HAM correspondant. L'Agent de support Data Protector peut communiquer directement avec le pilote .HAM afin d'accéder à l'adaptateur hôte SCSI. Par conséquent, vous devez installer le pilote de l'adaptateur hôte SCSI. Vous pouvez télécharger les

dernières versions des pilotes Adaptec à partir du site Web http://www.adaptec.com.

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

Exemple

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

```
SET RESERVED BUFFERS BELOW 16 MEG=200

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

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

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

REMARQUE :

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

CONSEIL :

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

```
SCAN FOR NEW DEVICES

SCAN ALL LUNS
```

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

Etape suivante

Une fois que le logiciel Agent général de support Data Protector est installé correctement sur la plate-forme Novell NetWare, il est conseillé de vérifier son installation. Reportez-vous à la section “Vérification de l'installation de l'Agent général de support sous Novell NetWare” à la page 464.

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

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

Vous pouvez installer l'Agent de disque, l'Agent général de support et l'interface utilisateur (interface de ligne de commande uniquement) de Data Protector sur des systèmes OpenVMS 7.3-2/IA64 8.2-1. Vous pouvez également installer le composant Intégration Oracle sur des systèmes utilisant OpenVMS I64 version 7.3-1 ou supérieure. Pour obtenir des informations sur les composants Data Protector, reportez-vous à la section “Composants Data Protector” à la page 77.

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

Pour des informations plus précises sur OpenVMS, consultez le document *OpenVMS Release Notes* disponible dans le répertoire des documents d'aide par défaut sous OpenVMS, par exemple : `SYS$COMMON:[SYSHLP]DPA0611.RELEASE_NOTES.`

Configuration système requise

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

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

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

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

1. Si vous disposez déjà d'un fichier d'installation PCSI, passez à l'Étape 2 à la page 143. Pour obtenir le fichier d'installation PCSI, montez le DVD-ROM d'installation sur un système OpenVMS Server et copiez le fichier à l'endroit désiré. Vous pouvez également utiliser FTP pour récupérer le fichier PCSI à partir d'un système Windows.
2. Exécutez la commande suivante :

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

   où `unité:[répertoire]` est l'emplacement du fichier d'installation .PCSI.
3. Vérifiez la version du kit en répondant `YES` à l'invite :

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

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

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

Exemple

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

COPYRIGHT HEWLETT-PACKARD COMPANY 2010

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

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

[YES] YES

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

[YES] YES

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

[YES] YES
```

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

[YES] YES

Do you want to review the options?

[NO] YES

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

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

YES

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

YES

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

YES

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

[YES] YES

Are you satisfied with these options?

[YES] YES
```

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 utilisateur graphique de Data Protector comme indiqué dans la section “Importation de clients dans une cellule ” à la page 222.

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

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

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

REMARQUE :

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

```
%PCSI-I-CANNOTVAL, cannot validate [PATH]HP-AXPVMS-DP-A0611
-XXX-1.PCSI;1 -PCSI-I-NOTSIGNED, product kit
is not signed and therefore has no manifest file
```

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

Installation dans un environnement de cluster

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

Si vous utilisez un nom d'alias TCP/IP pour le cluster, vous pouvez également définir un client pour le nom d'alias si vous utilisez un disque système commun pour le cluster. Lorsque le client alias est défini, il n'est plus nécessaire de configurer individuellement chaque nœud client. Vous avez alors le choix entre la définition du client et la définition de l'alias pour exécuter les sauvegardes et restaurations dans un cluster. Selon votre configuration, la sauvegarde ou la restauration peuvent ou non utiliser un chemin d'accès direct vers votre lecteur de bande ou votre bibliothèque de bandes.

Configuration de l'Agent de disque

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

- Les spécifications de fichier saisies dans l'interface utilisateur graphique ou transmises 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 utilisateur graphique ou dans l'interface de ligne de commande. Ajoutez les spécifications de fichier sous l'option `-only`, en utilisant des caractères génériques pour le numéro de version, comme suit :

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

Configuration de l'Agent de support

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

```
$ RUN SYS$SYSTEM:SYSMAN
```

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

où :

- c = K pour les bibliothèques de bandes SCSI à connexion directe.
- a = A,B,C, …lettre de l'adaptateur pour le contrôleur SCSI.

- n = numéro d'unité du robot de la bibliothèque de bandes.

REMARQUE :

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

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

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

REMARQUE :

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

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

Agent de support sur un cluster

Avec les périphériques reliés aux systèmes de cluster :

1. Configurez chaque lecteur et bibliothèque de bande pour qu'il puisse être accessible à partir de tous les nœuds.
2. Ajoutez le nom du nœud à la fin du nom du périphérique pour le différencier.
3. Pour les périphériques à bande, définissez un `nom de verrouillage de périphérique` dans `Devices/Properties/Settings/Advanced/Other`.

Exemple

Dans un cluster comportant les nœuds A et B, un TZ89 est connecté au nœud A et relié comme serveur au nœud B par protocole MSCP. Configurez un périphérique nommé `TZ89_A`, avec le nœud A comme client et configurez un périphérique nommé `TZ89_B`, avec le nœud B comme client. Les deux périphériques obtiennent le nom

de verrouillage de périphérique commun TZ89. Data Protector peut alors utiliser les périphériques par chacun des chemins d'accès, tout en les reconnaissant comme un périphérique unique. Si vous exécutez une sauvegarde sur le noeud B avec TZ89_A, Data Protector transfère les données du noeud B au périphérique sur le noeud A. Si vous exécutez une sauvegarde sur le noeud B avec TZ89_B, le serveur MSCP OpenVMS transfère au périphérique sur le noeud A les données du noeud B.

REMARQUE :

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

Interface de ligne de commande

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

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

Intégration Oracle

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

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

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

Etape suivante

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

Installation en local de clients UNIX et Mac OS X

Si aucun Serveur d'installation pour UNIX n'est installé 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 HP-UX ou Solaris et Linux.

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 77.

Conditions préalables

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

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

REMARQUE :

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

Procédure

Pour installer les clients UNIX et Mac OS X en local, procédez comme suit :

1. Insérez et montez le DVD-ROM d'installation HP-UX ou Solaris et Linux.

2. A partir de `Point_de_montage/LOCAL_INSTALL`, exécutez la commande `omnisetup.sh`.

   La syntaxe de la commande est la suivante :

   ```
   omnisetup.sh [-source répertoire] [-server nom] [-install
   liste_composants]
   ```

   où :

   - *`répertoire`* est l'emplacement où le DVD-ROM d'installation est monté. S'il n'est pas spécifié, le répertoire en cours est utilisé.
   - *`nom`* est un nom d'hôte complet du Gestionnaire de cellule de la cellule sur laquelle vous souhaitez installer le client. S'il n'est pas spécifié, le client ne sera pas automatiquement importé dans la cellule.

   REMARQUE :

   Si vous mettez à niveau le client qui ne réside pas sur le Gestionnaire de cellule, il n'est pas nécessaire de spécifier `-install liste_composants`. Dans ce cas, le programme d'installation sélectionnera sans émettre d'invite les mêmes composants que ceux déjà installés sur le système.

   Toutefois, pour mettre à niveau les composants du client se trouvant dans le Gestionnaire de cellule, exécutez la commande `omnisetup.sh` avec le paramètre `-install liste_composants` une fois la mise à niveau de Gestionnaire de cellule terminée.

   - *`liste_composants`* est une liste séparée par des virgules des codes composants à installer. L'utilisation d'espaces n'est pas autorisée. Si le paramètre `-install` n'est pas spécifié, le processus d'installation vous invite à installer séparément tous les composants disponibles sur le système.

   REMARQUE :

   Dans le cas d'une mise à niveau du client, si vous ne spécifiez pas le paramètre `-install`, le processus d'installation sélectionnera, sans émettre d'invite, les composants qui étaient installés sur le système avant le début de la mise à niveau.

   La liste des composants est présentée dans le tableau ci-dessous. La liste exacte des composants dépend de leur disponibilité sur ce système particulier.

Les composants sont décrits à la section “Composants Data Protector” à la page 77.

Tableau 7 Codes des composants Data Protector

Code composant	Composant
cc	Interface utilisateur
da	Agent de disque
ma	Agent de support général
ndmp	Agent de support NDMP
informix	Intégration Informix
lotus	Intégration Lotus
oracle	Intégration Oracle
vmware	Intégration VMware (hérité)
veagent	Intégration de l'environnement virtuel
ov	HP Network Node Manager
sybase	Intégration Sybase
sap	Intégration SAP R/3
sapdb	Intégration SAP DB
db2	Intégration DB2
emc	Agent EMC Symmetrix
ssea	HP StorageWorks Agent P9000 XP
smisa	HP StorageWorks Agent P6000 EVA SMI-S
vls_am	Auto-migration VLS

Code composant	Composant
javagui	Interface utilisateur graphique Java (interface utilisateur graphique, interface utilisateur du Manager-of-Managers)
docs	Documentation en anglais (guides, aide)
fra_ls	Documentation en français (guides, aide)
jpn_ls	Documentation en japonais (guides, aide)
chs_ls	Documentation en chinois simplifié (guides, aide)

Exemple

L'exemple ci-dessous présente l'installation des composants `Agent de disque`, `Agent général de support`, `Interface utilisateur` et `Intégration Informix` sur un client qui sera automatiquement importé dans la cellule avec le Gestionnaire de cellule `ordinateur.société.com` :

```
./omnisetup.sh -server anapola.company.com -install
da,ma,cc,informix
```

3. Le processus d'installation vous indique si l'installation est terminée et si le client a été importé dans la cellule Data Protector.

   Le composant `CORE` est installé la première fois qu'un composant logiciel est sélectionné pour l'installation.

   Le composant `CORE-INTEG` est installé la première fois qu'un composant du logiciel d'intégration est sélectionné pour l'installation ou la réinstallation.

Exécution de l'installation à partir du disque dur

Pour copier le DVD-ROM d'installation sur votre ordinateur et exécuter l'installation ou la mise à niveau des clients UNIX et Mac OS X à partir du disque dur, copiez au moins les répertoires `hpux/DP_DEPOT` ou `solaris/DP_DEPOT` et `LOCAL_INSTALL`.

REMARQUE :

Les dépôts Linux ne prennent pas en charge l'installation en local. Vous devez copier le dépôt HP-UX (si vous installez les clients à partir du DVD d'installation HP-UX) ou le dépôt Solaris (si vous opérez l'installation à partir du DVD d'installation Solaris et Linux), y compris sur les systèmes Linux. Cette limite ne s'applique pas si vous effectuez l'installation à partir du DVD.

Si, par exemple, vous copiez les packages d'installation dans `/var/dp62`, les répertoires doivent correspondre à un sous-répertoire de `/var/dp62` :

```
# pwd
/var/dp62
# ls
DP_DEPOT
LOCAL_INSTALL
```

Après avoir copié les données sur le disque dur, passez au répertoire `LOCAL_INSTALL` et exécutez la commande suivante :

```
omnisetup.sh [-server nom] [-install liste_composants]
```

Par exemple :

```
./omnisetup.sh -install da
```

Notez que si vous avez copié le répertoire `DP_DEPOT` dans un répertoire différent (en raison de contraintes relatives à l'espace disque, par exemple), l'option `-source` est également requise.

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 utilisateur graphique de Data Protector. Pour connaître la procédure à suivre, reportez-vous à la section “Importation de clients dans une cellule ” à la page 222. 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 Server ou Microsoft Exchange Server, avec Data Protector. Les intégrations ZDB Data Protector sont des composants logiciels permettant d'exécuter une sauvegarde avec temps d'indisponibilité nul ou une restauration instantanée via des baies de disques, telles que HP StorageWorks P6000 EVA Disk Array Family.

Les systèmes exécutant des applications de base de données sont appelés **clients d'intégration** ; les systèmes utilisant les baies de disques ZDB pour la sauvegarde et la restauration des données sont appelés **clients d'intégration ZDB**. Ces clients sont installés à l'aide de la même procédure que tout autre client sous Windows ou UNIX à condition que le composant logiciel approprié ait été sélectionné (par exemple, le composant `Intégration MS Exchange` pour la sauvegarde de la base de données Microsoft Exchange, le composant Agent `HP StorageWorks P6000 EVA SMI-S` pour une sauvegarde avec temps d'indisponibilité nul et une restauration instantanée avec HP StorageWorks P6000 EVA Disk Array Family, etc.).

Configuration système requise

- Pour connaître la configuration système requise, l'espace disque requis, les plates-formes, processeurs et composants Data Protector pris en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.
- Vous devez disposer d'une licence pour pouvoir utiliser l'intégration de Data Protector avec une application de base de données. Pour plus d'informations sur l'attribution des licences, reportez-vous à la section “Structure de produit et licences de Data Protector 6.20” à la page 358.
- 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 44 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 77.

Notez que dans les situations exposées ci-dessous, vous devez installer les composants Data Protector suivants :

- Le composant `Agent de disque` pour pouvoir sauvegarder des données de système de fichiers avec Data Protector. Vous pouvez utiliser l'Agent de disque dans les cas suivants :
  - Pour exécuter une sauvegarde du système de fichiers de données importantes pour lesquelles la sauvegarde de l'application de base de données *ne peut pas* être utilisée.
  - Pour exécuter un essai de sauvegarde du système de fichiers d'un serveur d'application de base de données (serveur Oracle ou MS SQL Server, par exemple). Vous devez procéder à un essai de sauvegarde de système de fichier *avant* de configurer l'intégration Data Protector avec une application de base de données et résoudre les problèmes - notamment de communication - liés à l'application et à Data Protector.
  - Pour exécuter une image disque et un client ZDB de système de fichiers.
  - Pour effectuer une restauration à partir d'un support de sauvegarde vers le système d'application sur le réseau LAN dans le cas d'intégrations ZDB SAP R/3.
- Le composant `Interface utilisateur` pour obtenir l'accès à l'interface utilisateur graphique et à l'interface de ligne de commande de Data Protector sur le client d'intégration de Data Protector.
- Le composant `Agent général de support` si des périphériques de sauvegarde sont connectés au client d'intégration Data Protector. Sur les clients Data Protector utilisés pour accéder à un lecteur dédié NDMP via le serveur NDMP, l'`Agent de support NDMP` est requis.

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

Pour plus d'informations sur des clients d'intégration spécifiques, reportez-vous aux paragraphes correspondants ci-après :

- "Clients Microsoft Exchange Server" à la page 160
- "Clients Microsoft SQL Server" à la page 162
- "Clients Microsoft SharePoint Server" à la page 163
- "Clients Microsoft Hyper-V" à la page 170
- "Clients Sybase" à la page 165
- "Clients Informix Server" à la page 165
- "Clients SAP R/3" à la page 166
- "Clients SAP MaxDB" à la page 167
- "Clients Oracle Server" à la page 167

- "Clients VMware" à la page 167
- "Clients DB2" à la page 171
- "Clients NNM" à la page 171
- "Clients de serveur NDMP" à la page 171
- "Clients Microsoft Volume Shadow Copy Service" à la page 172
- "Clients Lotus Notes/Domino Server" à la page 172
- "Intégration EMC Symmetrix" à la page 188
- "Intégration HP StorageWorks P9000 XP Disk Array Family" à la page 181
- "Intégration HP StorageWorks P6000 EVA Disk Array Family" à la page 173
- "Clients d'auto-migration VLS" à la page 195

Une fois que vous avez terminé l'installation du logiciel d'intégration Data Protector sur les clients d'intégration Data Protector comme la décrivent les sections indiquées, reportez-vous au *Guide d'intégration HP Data Protector*, au *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector* ou au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector pour configurer les clients d'intégration Data Protector*.

Installation en local

Si vous ne disposez d'aucun 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, HP-UX, ou Solaris et Linux, selon la plate-forme sur laquelle vous installez un client. Reportez-vous à la section "Installation de clients Windows" à la page 92 ou "Installation en local de clients UNIX et Mac OS X" à la page 151 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 222.

Installation distante

Vous devez installer le logiciel client à partir du Serveur d'installation pour UNIX sur les systèmes clients utilisant l'interface utilisateur graphique 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 83.

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 Data Protector P6000 EVA SMI-S`).

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 203.
- "Installation de Data Protector sur Microsoft Cluster Server" à la page 204.
- "Installation de clients Data Protector sur un cluster Veritas" à la page 216.
- "Installation de clients Data Protector sur un cluster Novell NetWare" à la page 217.
- "Installation de Data Protector sur un cluster IBM HACMP" à la page 220.

Pour plus d'informations sur la gestion de clusters, reportez-vous à l'index de l'aide en ligne (rubrique "cluster, MC/ServiceGuard") et au *Guide conceptuel HP Data Protector*.

Etape suivante

Une fois l'installation terminée, reportez-vous au *Guide d'intégration HP Data Protector* approprié pour plus d'informations sur la configuration de l'intégration.

Clients Microsoft Exchange Server

Les composants Data Protector à installer sur les systèmes Microsoft Exchange Server varient selon la solution de sauvegarde et de restauration que vous voulez utiliser. Vous avez le choix parmi les solutions suivantes :

- "Intégration de Data Protector avec Microsoft Exchange Server 2003/2007" à la page 161
- "Intégration de Data Protector avec Microsoft Exchange Server 2010" à la page 161

- "Intégration de Data Protector avec la boîte aux lettres Microsoft Exchange unique" à la page 162
- "Intégration de Data Protector avec Microsoft Volume Shadow Copy Service" à la page 162

Intégration de Data Protector avec Microsoft Exchange Server 2003/2007

Votre serveur Microsoft Exchange est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder les bases de données Microsoft Exchange, installez le composant `Intégration MS Exchange` sur le système Microsoft Exchange Server.

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.

Intégration de Data Protector avec Microsoft Exchange Server 2010

Votre environnement Microsoft Exchange Server 2010 est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder les bases de données Microsoft Exchange, veillez à installer les composants Data Protector suivants sur tous les systèmes Microsoft Exchange Server.

- `Intégration MS Exchange Server 2010`
- `Intégration MS Volume Shadow Copy`
- L'agent de baie de disques Data Protector approprié (si les données de Microsoft Exchange Server résident sur une baie de disques)

REMARQUE :

Pour les sessions de sauvegarde VSS transportable, le composant `Intégration MS Volume Shadow Copy` et l'agent de baie de disques Data Protector approprié doivent également être installés sur les systèmes de sauvegarde.

Dans les environnements DAG, le système virtuel DAG (hôte) doit également être importé dans la cellule Data Protector. Pour plus d'informations sur l'importation d'un client dans une cellule Data Protector, reportez-vous à l'index de l'aide en ligne : "importation, systèmes clients".

REMARQUE :

- Comme l'intégration de Data Protector avec Microsoft Exchange Server 2010 est basée sur la technologie VSS, le composant `Intégration MS Volume Shadow Copy` est installé automatiquement en même temps que le composant `Intégration MS Exchange Server 2010`. Si le composant `Intégration MS Volume Shadow Copy` est déjà installé, il fait l'objet d'une mise à niveau.
- Si vous supprimez le composant `Intégration MS Exchange Server 2010` d'un système, le composant `Intégration MS Volume Shadow Copy` n'est pas supprimé automatiquement. Notez également qu'il n'est pas possible de supprimer le composant `Intégration MS Volume Shadow Copy` d'un système sur lequel est installé le composant `Intégration MS Exchange Server 2010`.

Intégration de Data Protector avec la boîte aux lettres Microsoft Exchange unique

Votre serveur Microsoft Exchange doit être opérationnel.

Pour pouvoir sauvegarder la boîte aux lettres Microsoft Exchange et les éléments des dossiers publics, installez le composant `Intégration MS Exchange` sur le système Microsoft Exchange Server. Dans un environnement DAG, installez le composant sur tous les systèmes Microsoft Exchange Server inclus dans un DAG.

Sur des systèmes Microsoft Exchange Server 2007, vous devez installer un autre package pour permettre la fonctionnalité de l'intégration Microsoft Exchange Single Mailbox Data Protector. Ce package s'appelle Microsoft Exchange Server MAPI Client and Collaboration Data Objects (`ExchangeMapiCdo.EXE`) et vous pouvez le télécharger gratuitement à partir du site Web de Microsoft à l'adresse http://www.microsoft.com/downloads/Search.aspx?DisplayLang=en.

Intégration de Data Protector avec Microsoft Volume Shadow Copy Service

Reportez-vous à la section “Clients Microsoft Volume Shadow Copy Service” à la page 172.

Clients Microsoft SQL Server

Votre serveur Microsoft SQL Server est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données Microsoft SQL Server, vous devez sélectionner le composant `Intégration MS SQL` lors de la procédure d'installation.

Clients Microsoft SharePoint Server

Les composants Data Protector à installer dans un environnement Microsoft SharePoint Server varient selon la solution de sauvegarde et de restauration que vous voulez utiliser. Vous avez le choix parmi les solutions suivantes :

- "Intégration de Data Protector avec Microsoft SharePoint Server 2003" à la page 163
- "Intégration de Data Protector avec Microsoft SharePoint Server 2007/2010" à la page 163
- "Intégration de Data Protector avec la solution basée sur VSS Microsoft SharePoint Server 2007/2010" à la page 164
- "Intégration de Data Protector avec Microsoft Volume Shadow Copy Service" à la page 164
- "Extension de restauration granulaire de Data Protector pour Microsoft SharePoint Server" à la page 164

Intégration de Data Protector avec Microsoft SharePoint Server 2003

Les instances de Microsoft SharePoint Portal Server et les instances liées de Microsoft SQL Server doivent être opérationnelles.

Pour pouvoir sauvegarder des objets Microsoft SharePoint Portal Server, installez les composants Data Protector suivants :

- `Intégration MS SharePoint` - sur des systèmes Microsoft SharePoint Portal Server
- `Intégration MS SQL` - sur des systèmes Microsoft SQL Server

Intégration de Data Protector avec Microsoft SharePoint Server 2007/2010

Les instances de Microsoft SharePoint Server et les instances liées de Microsoft SQL Server doivent être opérationnelles.

Pour pouvoir sauvegarder des objets Microsoft SharePoint Server, installez les composants Data Protector suivants :

- `Intégration MS SharePoint 2007/2010` - sur les systèmes Microsoft SharePoint Server
- `Intégration MS SQL` - sur les systèmes Microsoft SQL Server

Intégration de Data Protector avec la solution basée sur VSS Microsoft SharePoint Server 2007/2010

Les instances de Microsoft SharePoint Server et les instances liées de Microsoft SQL Server doivent être opérationnelles.

Pour pouvoir sauvegarder des objets Microsoft SharePoint Server, installez les composants Data Protector suivants :

- `Intégration MS Volume Shadow Copy` - sur les systèmes Microsoft SQL Server et Microsoft SharePoint Server pour lesquels au moins l'un des services suivants est activé :

  Microsoft Office SharePoint Server 2007

  - `Base de données Windows SharePoint Services`
  - `Recherche d'aide Windows SharePoint Services`
  - `Recherche Office SharePoint Server`

  Microsoft SharePoint Server 2010

  - `Base de données SharePoint Foundation`
  - `Recherche d'aide SharePoint Foundation`
  - `Recherche SharePoint Server`

- Le composant `Interface utilisateur` sur l'un des serveurs Microsoft SharePoint équipés de l'`intégration MS Volume Shadow Copy` sur lequel vous prévoyez de configurer et lancer une sauvegarde.

Intégration de Data Protector avec Microsoft Volume Shadow Copy Service

Reportez-vous à la section "Clients Microsoft Volume Shadow Copy Service" à la page 172.

Extension de restauration granulaire de Data Protector pour Microsoft SharePoint Server

Les instances de Microsoft SharePoint Server et les instances liées de Microsoft SQL Server doivent être opérationnelles.

Pour pouvoir restaurer des objets Microsoft SharePoint Server individuels, installez l'`extension de restauration granulaire (GRE) MS SharePoint` sur le système Administration centrale de Microsoft SharePoint Server.

- Lors de l'installation du composant en local, l'assistant d'installation de Data Protector affiche la boîte de dialogue d'options GRE MS SharePoint. Indiquez le nom d'utilisateur et le mot de passe de l'administrateur de batterie de serveurs.
- Pour installer ce composant à distance, sélectionnez l'`extension de restauration granulaire MS SharePoint`, cliquez sur **Configurer**, puis indiquez le nom d'utilisateur et le mot de passe de l'administrateur de batterie de serveurs dans la boîte de dialogue d'options GRE MS SharePoint.

REMARQUE :

Vérifiez que les composants Data Protector nécessaires pour sauvegarder les données Microsoft SharePoint Server sont également installés dans l'environnement Microsoft SharePoint Server.

Clients Sybase

Votre serveur Sybase Backup Server est supposé sous tension et en cours de fonctionnement.

Pour sauvegarder la base de données Sybase, vous devez sélectionner les composants Data Protector suivants lors de la procédure d'installation :

- `Intégration Sybase` - pour la sauvegarde d'une base de données Sybase ;
- `Agent de disque` - installez l'Agent de disque pour deux raisons :
  - Pour exécuter une sauvegarde du système de fichiers de Sybase Backup Server. Effectuez cette sauvegarde *avant* de configurer votre intégration Data Protector Sybase et résolvez tous les problèmes liés à Sybase Backup Server et à Data Protector.
  - Pour exécuter une sauvegarde du système de fichiers de données importantes pour lesquelles Sybase Backup Server *ne peut pas* être utilisé.

Clients Informix Server

Votre serveur Informix Server est supposé sous tension et en cours de fonctionnement.

Pour sauvegarder la base de données Informix Server, vous devez sélectionner les composants Data Protector suivants lors de la procédure d'installation :

- `Intégration Informix` - pour la sauvegarde d'une base de données Informix Server ;
- `Agent de disque` - installez l'Agent de disque pour deux raisons :

- Pour exécuter une sauvegarde du système de fichiers Informix Server. Effectuez cette sauvegarde *avant* de configurer votre intégration Data Protector Informix Server et résolvez tous les problèmes liés à Informix Server et à Data Protector.
- Pour exécuter une sauvegarde du système de fichiers portant sur les données Informix Server importantes (telles que le fichier ONCONFIG, le fichier `sqlhosts`, le fichier d'amorçage de secours ON-Bar, `oncfg_INFORMIXSERVER.SERVERNUM`, les fichiers de configuration, etc.) qui *ne peuvent pas* être sauvegardés avec ON-Bar.

IBM HACMP Cluster

Si Informix Server est installé dans l'environnement de cluster IBM HACMP, installez le composant `Intégration Informix` sur tous les noeuds du cluster.

Clients SAP R/3

Configuration système requise

- Vérifiez que les logiciels Oracle suivants sont installés et configurés :
  - Oracle Enterprise Server (RDBMS) ;
  - logiciel Oracle Net8 ;
  - SQL*Plus.
- Votre serveur SAP R/3 Database est supposé sous tension et en cours de fonctionnement.

REMARQUE :

Les spécifications de sauvegarde de l'intégration SAP R/3 Data Protector sont entièrement compatibles avec la version antérieure de Data Protector. Data Protector exécute toutes les spécifications de sauvegarde créées par les versions antérieures. En revanche, vous ne pouvez pas utiliser sur une version antérieure de Data Protector les spécifications de sauvegarde créées avec la version actuelle.

Pour pouvoir sauvegarder la base de données SAP R/3, sélectionnez les composants suivants lors de la procédure d'installation :

- `Intégration SAP R/3`
- `Agent de disque`

Data Protector requiert l'installation d'un Agent de disque sur les serveurs de sauvegarde (clients comportant des données de système de fichiers à sauvegarder).

Clients SAP MaxDB

Votre serveur SAP MaxDB doit être opérationnel.

Pour pouvoir sauvegarder la base de données SAP MaxDB, vous devez sélectionner les composants Data Protector suivants lors de la procédure d'installation :

- `Intégration SAP DB` - pour pouvoir exécuter une sauvegarde en ligne intégrée d'une base de données SAP MaxDB
- `Agent de disque` - pour pouvoir exécuter une sauvegarde hors ligne non intégrée d'une base de données SAP MaxDB

Clients Oracle Server

Votre serveur Oracle est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données Oracle, vous devez sélectionner le composant `Intégration Oracle` lors de la procédure d'installation.

HP OpenVMS

Sous OpenVMS, après avoir installé l'intégration Oracle et l'avoir configurée selon les indications du *Guide d'intégration HP Data Protector pour Oracle et SAP*, vérifiez que l'entrée `-key Oracle8` figure dans `OMNI$ROOT:[CONFIG.CLIENT]omni_info`, par exemple :

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

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

Clients VMware

Les composants Data Protector à installer sur des systèmes VMware varient selon la solution de sauvegarde et de restauration que vous voulez utiliser. Vous avez le choix parmi les solutions suivantes :

- “Intégration de l'environnement virtuel Data Protector” à la page 168
- “Intégration VMware (hérité) Data Protector” à la page 168

- “Extension de restauration granulaire Data Protector pour VMware vSphere” à la page 169

Intégration de l'environnement virtuel Data Protector

Les hôtes de sauvegarde doivent être opérationnels.

Installez le composant `Intégration de l'environnement virtuel` Data Protector sur chaque système à utiliser comme hôte de sauvegarde.

Intégration VMware (hérité) Data Protector

Les systèmes VirtualCenter Server (le cas échéant) et ESX Server doivent être opérationnels. Pour pouvoir installer les clients VMware à distance, vous devez d'abord définir OpenSSH. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "installation, systèmes clients".

Installez le composant Data Protector `Intégration VMware (hérité)` sur les clients suivants :

- Tous les systèmes ESX Server à partir desquels vous prévoyez de sauvegarder des machines virtuelles
- Systèmes VirtualCenter (le cas échéant)
- Systèmes de sauvegarde proxy (si vous envisagez d'utiliser les méthodes de sauvegarde **VCBfile** et **VCBimage**)
- Systèmes Windows (physiques ou virtuels) sur lesquels vous prévoyez de restaurer des systèmes de fichiers de machines virtuelles

REMARQUE :

Le composant Data Protector `Intégration VMware (hérité)` ne peut pas être installé sur des systèmes ESXi Server. Par conséquent, certaines des fonctions de sauvegarde et restauration ne sont pas disponibles pour les machines virtuelles fonctionnant sur les systèmes ESXi Server.

Clusters

Installez le composant `Intégration VMware (hérité)` sur les deux noeuds de cluster, sans tenir compte de la présence de systèmes ESX Server ou VirtualCenter dans un cluster.

Extension de restauration granulaire Data Protector pour VMware vSphere

Le composant Data Protector Intégration de l'environnement virtuel doit être installé et configuré selon la procédure indiquée dans le *Guide d'intégration HP Data Protector pour les environnements de virtualisation*. Par ailleurs, les outils VMware version 4.x ou supérieure doivent être installés sur les machines virtuelles sur lesquelles vous envisagez de planifier des restaurations.

Limites

- Seule l'installation à distance de l'extension de restauration granulaire Data Protector pour VMware est prise en charge.

Sur le système proxy de montage, installez les composants Data Protector ci-dessous à distance. Pour plus d'informations, reportez-vous à l'index de l'aide en ligne : "installation, systèmes clients".

- `Interface utilisateur`
- `Intégration de l'environnement virtuel`
- `Agent de l'extension de restauration granulaire VMware`

Sur le système Virtual Center (vCenter) Server, procédez comme suit :

1. Installez le composant `Plug-in Web de l'extension de restauration granulaire VMware` à distance.
2. Importez le système vCenter Server vers la cellule Data Protector avec un type **VMware vCenter** au moyen de l'interface utilisateur graphique de Data Protector. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "importation, systèmes clients".

REMARQUE :

Si le composant Intégration de l'environnement virtuel est installé sur le système vCenter Server, vous ne pouvez pas installer à distance d'autres composants Data Protector sur ce système. Dans ce cas, pour installer le composant Plug-in Web de l'extension de restauration granulaire VMware sur ce système vCenter Server, procédez comme suit :

1. Importez le système vCenter Server vers la cellule Data Protector avec un type **Client Data Protector**.
2. Importez le système vCenter Server vers la cellule Data Protector avec un type **VMware vCenter**.
3. Installez le composant `Plug-in Web de l'extension de restauration granulaire VMware` à distance.

Clients Microsoft Hyper-V

Les composants Data Protector à installer sur les systèmes Microsoft Hyper-V varient selon la solution de sauvegarde et de restauration que vous voulez utiliser. Vous avez le choix parmi les solutions suivantes :

- "Intégration de l'environnement virtuel Data Protector" à la page 168
- "Intégration de Data Protector avec Microsoft Volume Shadow Copy Service" à la page 170

Intégration de l'environnement virtuel Data Protector

Les hôtes de sauvegarde et les systèmes Microsoft Hyper-V à utiliser pour la sauvegarde ou la restauration doivent être opérationnels.

installez les composants Data Protector suivants sur les hôtes de sauvegarde et les systèmes Microsoft Hyper-V :

- `Intégration de l'environnement virtuel`
- `Intégration MS Volume Shadow Copy`

Intégration de Data Protector avec Microsoft Volume Shadow Copy Service

Pour plus d'informations concernant les composants à installer sur les systèmes Microsoft Hyper-V, reportez-vous à la section "Clients Microsoft Volume Shadow Copy Service" à la page 172.

Clients DB2

Votre serveur DB2 est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données DB2, vous devez sélectionner les composants `Intégration DB2` et `Agent de disque` lors de la procédure d'installation.

Dans un environnement à partition physique, installez les composants `Intégration DB2` et `Agent de disque` sur chaque nœud physique (système) sur lequel réside la base de données.

REMARQUE :

Connectez-vous comme utilisateur `root` pour effectuer l'installation.

Clients NNM

Votre système NNM est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données NNM, vous devez sélectionner les composants `Intégration de sauvegarde HP NNM` et `Agent de disque` lors de la procédure d'installation. Vous aurez besoin de l'Agent de disque pour exécuter les scripts antérieurs et postérieurs à la sauvegarde utilisés pour les opérations de sauvegarde.

Clients de serveur NDMP

Votre serveur NDMP est supposé sous tension et en cours de fonctionnement.

Au cours de la procédure d'installation, sélectionnez l'`Agent de support NDMP` et installez-le sur tous les clients Data Protector ayant accès aux lecteurs NDMP dédiés.

REMARQUE :

Dans le cas où un client Data Protector ne doit pas être utilisé pour accéder à un lecteur NDMP dédié par le serveur NDMP et sera uniquement utilisé pour commander le robot de la bibliothèque, on peut installer sur ce client soit l'`Agent de support NDMP`, soit l'`Agent général de support`.

Notez que seul un Agent de support peut être installé sur un client Data Protector.

Clients Microsoft Volume Shadow Copy Service

Pour sauvegarder les modules d'écriture VSS ou uniquement le système de fichiers avec VSS, installez les composants logiciels Data Protector suivants sur le système d'application (*sauvegarde locale*) ou à la fois sur le système d'application et le système de sauvegarde (*sauvegarde transportable*) :

- `Intégration MS Volume Shadow Copy`.
- Si vous utilisez une baie de disques (avec des fournisseurs matériels), l'agent de baie de disques approprié (`Agent HP StorageWorks P6000 EVA SMI-S`, `Agent HP StorageWorks P9000 XP` ou `Agent HP StorageWorks P4000`).

Une fois que vous avez installé l'intégration VSS, vous devez résoudre les volumes sources sur le système d'application pour effectuer des sessions de sauvegarde ZDB sur disque et ZDB sur disque + bande (sessions avec restauration instantanée). Effectuez l'opération de résolution à partir de n'importe quel client VSS de la cellule, en procédant comme suit :

```
omnidbvss –resolve {–apphost ApplicationSystem | –all}
```

Si vous ne procédez pas à la résolution du système d'application ou bien si la résolution échoue, le système d'application est automatiquement résolu si la variable `OB2VSS_DISABLE_AUTO_RESOLVE` dans le fichier `omnirc` a la valeur `0` (par défaut). Dans ce cas, la durée de la sauvegarde pour la création d'une réplique est prolongée.

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

Clients Lotus Notes/Domino Server

Votre serveur Lotus Notes/Domino Server est supposé sous tension et en cours de fonctionnement.

Pour pouvoir sauvegarder la base de données Lotus Notes/Domino Server, vous devez sélectionner les composants `Intégration Lotus` et `Agent de disque` lors de la procédure d'installation. Vous avez besoin du composant `Agent de disque` pour pouvoir sauvegarder les données du système de fichiers avec Data Protector pour les tâches suivantes :

- Sauvegarde des données importantes qui *ne peuvent* être sauvegardées avec l'agent d'intégration Lotus. Il s'agit de fichiers "non-bases de données", qui doivent

être sauvegardés pour fournir une solution complète de protection des données pour un serveur Lotus Domino R5, par exemple `notes.ini`, `desktop.dsk` et tous les fichiers `*.id`.

- Essai de sauvegarde du système de fichiers pour résoudre les problèmes - notamment de communication - liés à l'application et à Data Protector.

Cluster Lotus Domino

Installez les composants `Intégration Lotus` et `Agent de disque` sur les serveurs Domino qui seront utilisés pour la sauvegarde et, si vous envisagez de restaurer des bases de données Domino sur d'autres serveurs Domino contenant des répliques de ces bases, installez également les composants sur ces serveurs.

Intégration HP StorageWorks P6000 EVA Disk Array Family

Pour intégrer HP StorageWorks P6000 EVA Disk Array Family avec Data Protector, installez les composants logiciels Data Protector suivants sur les systèmes d'application et de sauvegarde :

- `HP StorageWorks P6000 EVA Agent SMI-S`
- `Agent général de support`

  Installez le composant `Agent général de support` sur le système de sauvegarde pour sauvegarder les données en bloc. Installez-le sur le système d'application pour sauvegarder les journaux d'archive ou pour restaurer le système.

- `Agent de disque`

  Installez le composant `Agent de disque` sur les systèmes d'application et de sauvegarde pour exécuter des sauvegardes ZDB d'image disque et de système de fichiers. Les clients sans Agent de disque ne sont pas répertoriés dans les listes déroulantes `Système d'application` et `Système de sauvegarde` lors de la création d'une spécification de sauvegarde ZDB.

IMPORTANT :

Sur les systèmes Microsoft Windows Server 2008, deux correctifs spécifiques Windows Server 2008 doivent être installés pour permettre le fonctionnement normal de l'intégration Data Protector HP StorageWorks P6000 EVA Disk Array Family. Vous pouvez télécharger les packages correctifs requis à partir des sites Web de Microsoft http://support.microsoft.com/kb/952790.

Installation sur un cluster

Vous pouvez installer l'intégration HP StorageWorks P6000 EVA Disk Array Family dans un environnement de cluster. Pour connaître les configurations de clusters prises en charge et la configuration requise pour l'installation, reportez-vous au *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Intégration à d'autres applications

Pour installer l'intégration HP StorageWorks P6000 EVA Disk Array Family avec une application de base de données, installez le composant Data Protector spécifique pour l'intégration sur les systèmes d'application et de sauvegarde, et effectuez les tâches d'installation pertinentes pour cette intégration. Vous pouvez installer l'intégration HP StorageWorks P6000 EVA Disk Array Family avec Oracle Server, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server et Microsoft Volume Shadow Copy Service.

Intégration de HP StorageWorks P6000 EVA Disk Array Family avec Oracle Server

Configuration système requise

- Les logiciels suivants doivent être installés et configurés sur le système d'application et sur le système de sauvegarde pour la méthode de jeu de sauvegarde ZDB :
  - Oracle Enterprise Server (RDBMS) ;
  - Services Oracle Net ;
  - SQL*Plus.

  Le logiciel Oracle installé sur le système de sauvegarde doit l'être dans le même répertoire que sur le système d'application. Les binaires doivent être identiques à ceux du système d'application. Vous pouvez y parvenir en copiant les fichiers et l'environnement système du système d'application vers le système de sauvegarde ou par une installation "propre" des binaires Oracle sur le système de sauvegarde avec les mêmes paramètres d'installation que sur le système d'application.
- Les fichiers de base de données Oracle du système d'application doivent être installés sur les volumes source qui seront dupliqués à l'aide de l'agent SMI-S que vous avez installé.

  Selon l'emplacement du fichier de contrôle Oracle, des fichiers journaux de rétablissement en ligne et du fichier SPFILE, les deux options suivantes sont possibles :

- Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE résident sur un groupe de volumes (si LVM est utilisé) ou un volume source **différent** des fichiers de données Oracle.

  La restauration instantanée est activée par défaut dans ce type de configuration.

- Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE résident sur le **même** groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle.

  Par défaut, la restauration instantanée *n'est pas* activée dans ce type de configuration. Vous pouvez l'activer en définissant les variables `omnirc` `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Pour plus d'informations, reportez-vous au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Les fichiers journaux de rétablissement archivés Oracle ne doivent pas nécessairement résider sur des volumes source.

Si certains des fichiers de données Oracle sont installés sur des liens symboliques, vous devez créer ces liens également sur le système de sauvegarde.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez la base de données du catalogue de récupération Oracle. De préférence, installez-la sur un autre système, sur des disques qui ne sont pas en miroir. Laissez le catalogue de récupération non enregistré. Pour plus d'informations sur l'installation de la base de données, reportez-vous à la documentation Oracle.

2. Installez les composants logiciels Data Protector suivants :
   - `HP StorageWorks Agent P6000 EVA SMI-S` – sur le système d'application et le système de sauvegarde
   - `Intégration Oracle` – sur le système d'application et le système de sauvegarde

REMARQUE :

- Le composant `Intégration Oracle` Data Protector sur le système de sauvegarde n'est nécessaire que pour la méthode de jeu de sauvegarde ZDB. Il n'est pas nécessaire pour la méthode proxy-copy ZDB.
- Dans un environnement de cluster RAC, plusieurs instances Oracle accèdent à la base de données d'application Oracle. Par conséquent, installez les composants Data Protector `Intégration Oracle` et `Agent HP StorageWorks P6000 EVA SMI-S` sur tous les systèmes exécutant les instances Oracle.
- Si vous avez installé la base de données du catalogue de récupération Oracle sur un autre système, il n'est pas nécessaire d'y installer des composants logiciels Data Protector.

Intégration de HP StorageWorks P6000 EVA Disk Array Family avec SAP R/3

Configuration système requise

- Les logiciels Oracle suivants doivent être installés sur le système d'application.
  - Oracle Enterprise Server (RDBMS) ;
  - Services Oracle Net ;
  - SQL*Plus.
- Si vous envisagez d'exécuter des sessions ZDB compatibles SAP (BRBACKUP démarré sur le système de sauvegarde et non sur le système d'application), le système de sauvegarde doit être configuré. Pour plus de détails, reportez-vous au guide de la base de données SAP pour Oracle (sauvegarde split mirror, configuration du logiciel).
- La base de données du système d'application peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers.
  - Les fichiers de données Oracle *doivent* résider sur une baie de disques.

- Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas nécessairement résider sur une baie de disques. En revanche, pour les sessions ZDB *en ligne* compatibles SAP, les fichiers de contrôle doivent résider sur une baie de disques.
- Pour la *sauvegarde hors ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* résider sur une baie de disques.
- Les fichiers journaux de rétablissement archivés ne doivent pas nécessairement résider sur une baie de disques.

Si le fichier de contrôle Oracle, les journaux de rétablissement en ligne et le fichier SPFILE Oracle résident sur le *même* groupe de volume LVM ou volume source que les fichiers de données Oracle, définissez les variables `ZDB_ORA_NO_CHECKCONF_IR`, `ZDB_ORA_INCLUDE_CF_OLF` et `ZDB_ORA_INCLUDE_SPF` de la commande `omnirc` Data Protector. Sinon, vous ne pourrez pas exécuter de sessions de sauvegarde ZDB sur disque et ZDB sur disque + bande. Pour plus d'informations, reportez-vous au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

REMARQUE :

Si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez les liens également sur le système de sauvegarde.

UNIX seulement : Si la base de données Oracle est installée sur des partitions brutes (image disque ou volumes logiques bruts), vérifiez que les noms de volume/groupe de disques sont identiques sur le système d'application et le système de sauvegarde.

- Sous UNIX, vérifiez que les utilisateurs suivants sont définis sur le système d'application :
  - `oraORACLE_SID` dans le groupe principal `dba`
  - `ORACLE_SIDadm` dans le groupe UNIX `sapsys`
- Le logiciel SAP R/3 doit être correctement installé sur le système d'application.

  Les répertoires standard suivants doivent être installés sur le système d'application après l'installation de SAP R/3 :

REMARQUE :

L'emplacement des répertoires dépend des variables d'environnement (systèmes UNIX) ou de registre (systèmes Windows). Reportez-vous à la documentation SAP R/3 pour plus d'informations.

- `ORACLE_HOME/dbs` (systèmes UNIX) *`ORACLE_HOME`*`\database` (systèmes Windows) - les profils Oracle et SAP)
- `ORACLE_HOME/bin` (systèmes UNIX) *`ORACLE_HOME`*`\bin` (systèmes Windows) - les fichiers binaires Oracle
- SAPDATA_HOME`/sapbackup` (systèmes UNIX) *`SAPDATA_HOME`*`\sapbackup` (systèmes Windows) - le répertoire SAPBACKUP avec fichiers journaux BRBACKUP
- SAPDATA_HOME`/sapbarch` (systèmes UNIX) SAPDATA_HOME`\sapbarch` (systèmes Windows) - le répertoire SAPARCH avec fichiers journaux BRARCHIVE
- SAPDATA_HOME`/sapreorg` (systèmes UNIX) *`SAPDATA_HOME`*`\sapreorg` (systèmes Windows)
- SAPDATA_HOME`/sapcheck` (systèmes UNIX) *`SAPDATA_HOME`*`\sapcheck` (systèmes Windows)
- SAPDATA_HOME`/saptrace` (systèmes UNIX) SAPDATA_HOME`\saptrace` (systèmes Windows)
- `/usr/sap/ORACLE_SID/SYS/exe/run` (systèmes UNIX)
  `c:\Oracle\ORACLE_SID\sys\exe\run` (systèmes Windows)

REMARQUE :

Si vous envisagez d'effectuer une restauration instantanée, vérifiez que les répertoires `sapbackup`, `saparch` et `sapreorg` figurent sur d'autres volumes source que les fichiers de données Oracle.

Systèmes UNIX

Sur les systèmes UNIX, si les six derniers répertoires ne sont pas aux emplacements indiqués ci-dessus, créez les liens appropriés vers eux.

Sur les systèmes UNIX, le propriétaire du répertoire `/usr/sap/ORACLE_SID/SYS/exe/run` doit être l'utilisateur UNIX `ora`*`ORACLE_SID`*. Le propriétaire des

fichiers SAP R/3 doit être l'utilisateur UNIX `ora`*`ORACLE_SID`* et le groupe UNIX `dba` avec le bit setuid à 1 (chmod 4755 ...). L'exception est le fichier BRRESTORE, dont le propriétaire doit être l'utilisateur UNIX *`ORACLE_SID`*`adm`.

Exemple UNIX

Si *`ORACLE_SID`* est PRO, les droits à l'intérieur du répertoire `/usr/sap/PRO/SYS/exe/run` doivent ressembler à ce qui suit :

```
-rwsr-xr-x   1 orapro dba 4598276 Apr 17  2010 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2010 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2010 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2010


brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  2010 brtools
```

Procédure d'installation

1. Installez SAP R/3 BRTOOLS sur le système d'application.
2. Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :
   - `Agent HP StorageWorks P6000 EVA SMI-S`
   - `Intégration SAP R/3`
   - `Agent de disque`

REMARQUE :

Il n'est pas nécessaire d'installer `Intégration SAP R/3` sur le système de sauvegarde si vous envisagez d'exécuter des sessions ZDB compatibles SAP lors desquelles BRBACKUP est démarré sur ce système.

Sur les systèmes Windows, les composants logiciels de Data Protector doivent être installés avec le compte administrateur SAP R/3, et ce groupe doit être inclus dans le groupe local `ORA_DBA` ou `ORA_SID_DBA` sur le système où l'instance SAP R/3 est exécutée.

Intégration de HP StorageWorks P6000 EVA Disk Array Family 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 P6000 EVA SMI-S` – sur les systèmes d'application et de sauvegarde
- `Intégration MS Exchange` – sur le système d'application uniquement

Intégration de HP StorageWorks P6000 EVA Disk Array Family avec MS SQL

Condition préalable

Microsoft SQL Server doit être installé sur le système d'application. Les bases de données utilisateur *doivent* résider sur les volumes sources de la baie de disques, tandis que les bases de données système peuvent être installées n'importe où. Cependant, si les bases de données système sont elles aussi installées sur la baie de disques, elles *doivent* l'être sur des volumes 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 P6000 EVA SMI-S` – sur les systèmes d'application et de sauvegarde
- `Intégration MS SQL` – sur le système d'application uniquement

Intégration HP StorageWorks P9000 XP Disk Array Family

Pour intégrer HP StorageWorks P9000 XP Disk Array Family avec Data Protector, installez les composants logiciels Data Protector suivants sur les systèmes d'application et de sauvegarde :

- `Agent HP StorageWorks P9000 XP`
- `Agent général de support`

  Installez le composant `Agent général de support` sur le système de sauvegarde pour sauvegarder les données en bloc. Installez-le sur le système d'application pour sauvegarder les journaux d'archive ou pour restaurer le système.

- `Agent de disque`

  Installez le composant `Agent de disque` sur les systèmes d'application et de sauvegarde pour exécuter des sauvegardes ZDB d'image disque et de système de fichiers. Les clients sans Agent de disque ne sont pas répertoriés dans les listes déroulantes `Système d'application` et `Système de sauvegarde` lors de la création d'une spécification de sauvegarde ZDB.

IMPORTANT :

Sur les systèmes Microsoft Windows Server 2008, deux correctifs spécifiques Windows Server 2008 doivent être installés pour permettre le fonctionnement normal de l'intégration Data Protector HP StorageWorks P9000 XP Disk Array Family. Vous pouvez télécharger ces correctifs sur les sites de Microsoft http://support.microsoft.com/kb/952790 et http://support.microsoft.com/kb/973928.

Installation sur un cluster

Vous pouvez installer l'intégration HP StorageWorks P9000 XP Disk Array Family dans un environnement de cluster. Pour connaître les configurations de clusters prises en charge et la configuration requise pour l'installation, reportez-vous au *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Intégration à d'autres applications

Si vous voulez installer l'intégration HP StorageWorks P9000 XP Disk Array Family avec une application de base de données, installez le composant Data Protector spécifique pour l'intégration sur les systèmes d'application et de sauvegarde, et

effectuez les tâches d'installation pertinentes pour cette intégration. Vous pouvez installer l'intégration HP StorageWorks P9000 XP Disk Array Family avec Oracle Server, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server et Microsoft Volume Shadow Copy Service.

Intégration de HP StorageWorks P9000 XP Disk Array Family avec Oracle Server

Conditions préalables

- Les logiciels suivants doivent être installés et configurés sur le système d'application et sur le système de sauvegarde pour la méthode de jeu de sauvegarde ZDB :
  - Oracle Enterprise Server (RDBMS) ;
  - Services Oracle Net ;
  - SQL*Plus.

  Le logiciel Oracle installé sur le système de sauvegarde doit l'être dans le même répertoire que sur le système d'application. Les binaires doivent être identiques à ceux du système d'application. Vous pouvez y parvenir en copiant les fichiers et l'environnement système du système d'application vers le système de sauvegarde ou par une installation "propre" des binaires Oracle sur le système de sauvegarde avec les mêmes paramètres d'installation que sur le système d'application.
- Les fichiers de données Oracle sur le système d'application doivent être installés sur des LDEV HP StorageWorks P9000 XP Disk Array Family mis en miroir sur le système de sauvegarde.

  Dans le cas de la méthode de jeu de sauvegarde, si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez ces liens également sur le système de sauvegarde.

  Selon l'emplacement du fichier de contrôle Oracle, des fichiers journaux de rétablissement en ligne et du fichier SPFILE, les deux options suivantes sont possibles :
  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE résident sur un groupe de volumes (si LVM est utilisé) ou un volume source **différent** des fichiers de données Oracle.

    La restauration instantanée est activée par défaut dans ce type de configuration.
  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et le fichier SPFILE résident sur le **même** groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle.

Par défaut, la restauration instantanée *n'est pas* activée dans ce type de configuration. Vous pouvez l'activer en définissant les variables `omnirc` `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Pour plus d'informations, reportez-vous au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Les fichiers journaux de rétablissement archivés Oracle ne doivent pas nécessairement résider sur des volumes source.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez la base de données du catalogue de récupération Oracle. De préférence, installez-la sur un autre système, sur des disques qui ne sont pas en miroir. Laissez le catalogue de récupération non enregistré. Pour plus d'informations sur l'installation de la base de données, reportez-vous à la documentation Oracle.
2. Installez les composants logiciels Data Protector suivants :
   - `Agent HP StorageWorks P9000 XP` – sur le système d'application et le système de sauvegarde
   - `Intégration Oracle` – sur le système d'application et le système de sauvegarde

REMARQUE :

- Le composant `Intégration Oracle` Data Protector sur le système de sauvegarde n'est nécessaire que pour la méthode de jeu de sauvegarde ZDB. Il n'est pas nécessaire pour la méthode proxy-copy ZDB.
- Dans un environnement de cluster RAC, plusieurs instances Oracle accèdent à la base de données d'application Oracle. Par conséquent, installez les composants Data Protector `Intégration Oracle` et `Agent HP StorageWorks P9000 XP` sur tous les systèmes exécutant les instances Oracle.
- Si vous avez installé la base de données du catalogue de récupération Oracle sur un autre système, il n'est pas nécessaire d'y installer des composants logiciels Data Protector.

Intégration de HP StorageWorks P9000 XP Disk Array Family avec SAP R/3

Configuration système requise

- Les logiciels Oracle suivants doivent être installés sur le système d'application :
  - Oracle Enterprise Server (RDBMS) ;
  - Services Oracle Net ;
  - SQL*Plus.
- Si vous envisagez d'exécuter des sessions ZDB compatibles SAP (BRBACKUP démarré sur le système de sauvegarde et non sur le système d'application), le système de sauvegarde doit être configuré. Pour plus de détails, reportez-vous au guide de la base de données SAP pour Oracle (sauvegarde split mirror, configuration du logiciel).
- La base de données du système d'application peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers.
  - Les fichiers de données Oracle *doivent* résider sur une baie de disques.
  - Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas nécessairement résider sur une baie de disques. En revanche, pour les sessions ZDB *en ligne* compatibles SAP, les fichiers de contrôle doivent résider sur une baie de disques.
  - Pour la *sauvegarde hors ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* résider sur une baie de disques.
  - Les fichiers journaux de rétablissement archivés ne doivent pas nécessairement résider sur une baie de disques.

  Si le fichier de contrôle Oracle, les journaux de rétablissement en ligne et le fichier SPFILE Oracle résident sur le *même* groupe de volume LVM ou volume source que les fichiers de données Oracle, définissez les variables `ZDB_ORA_NO_CHECKCONF_IR`, `ZDB_ORA_INCLUDE_CF_OLF` et `ZDB_ORA_INCLUDE_SPF` de la commande `omnirc` Data Protector. Sinon, vous ne pourrez pas exécuter de sessions de sauvegarde ZDB sur disque et ZDB sur disque + bande. Pour plus d'informations, reportez-vous au *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

REMARQUE :

Si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez les liens également sur le système de sauvegarde.

UNIX seulement : Si la base de données Oracle est installée sur des partitions brutes (image disque ou volumes logiques bruts), vérifiez que les noms de volume/groupe de disques sont identiques sur le système d'application et le système de sauvegarde.

- Sous UNIX, vérifiez que les utilisateurs suivants sont définis sur le système d'application :
  - `ora`*`ORACLE_SID`* dans le groupe principal `dba`
  - *`ORACLE_SID`*`adm` dans le groupe UNIX `sapsys`
- Le logiciel SAP R/3 doit être correctement installé sur le système d'application.

  Les répertoires standard suivants doivent être installés sur le système d'application après l'installation de SAP R/3 :

REMARQUE :

L'emplacement des répertoires dépend des variables d'environnement (systèmes UNIX) ou de registre (systèmes Windows). Reportez-vous à la documentation SAP R/3 pour plus d'informations.

  - *`ORACLE_HOME`*`/dbs` (systèmes UNIX)

    `ORACLE_HOME``\database` (systèmes Windows - les profils Oracle et SAP R/3)
  - *`ORACLE_HOME`*`/bin ou` (systèmes UNIX)

    `ORACLE_HOME``\bin` (systèmes Windows) - les fichiers binaires Oracle
  - SAPDATA_HOME`/sapbackup` (systèmes UNIX)

    `SAPDATA_HOME``\sapbackup` (systèmes Windows) - le répertoire SAPBACKUP des fichiers journaux BRBACKUP
  - *`SAPDATA_HOME`*`/saparch` (systèmes UNIX)

    `SAPDATA_HOME``\saparch` (systèmes Windows) - le répertoire SAPARCH des fichiers journaux BRARCHIVE
  - SAPDATA_HOME`/sapreorg` (systèmes UNIX)

SAPDATA_HOME\sapreorg (systèmes Windows)

- SAPDATA_HOME/sapcheck (systèmes UNIX)
  SAPDATA_HOME\sapcheck (systèmes Windows)
- SAPDATA_HOME/saptrace (systèmes UNIX)
  SAPDATA_HOME\saptrace (systèmes Windows)
- /usr/sap/ORACLE_SID/SYS/exe/run (systèmes UNIX)
  c:\Oracle\ORACLE_SID\sys\exe\run (systèmes Windows)

REMARQUE :

Si vous envisagez d'effectuer une restauration instantanée, vérifiez que les répertoires sapbackup, saparch et sapreorg figurent sur d'autres volumes source que les fichiers de données Oracle.

Systèmes UNIX

Sur les systèmes UNIX, si les six derniers répertoires ne sont pas aux emplacements indiqués ci-dessus, créez les liens appropriés vers eux.

Sur les systèmes UNIX, le propriétaire du répertoire /usr/sap/ORACLE_SID/SYS/exe/run doit être l'utilisateur UNIX ora*ORACLE_SID*. Le propriétaire des fichiers SAP R/3 doit être l'utilisateur UNIX ora*ORACLE_SID* et le groupe UNIX dba avec le bit setuid à 1 (chmod 4755 ...). L'exception est le fichier BRRESTORE, dont le propriétaire doit être l'utilisateur UNIX *ORACLE_SID*adm.

Exemple UNIX

Si *ORACLE_SID* est PRO, les droits à l'intérieur du répertoire /usr/sap/PRO/SYS/exe/run doivent ressembler à ce qui suit :

```
-rwsr-xr-x   1 orapro dba 4598276 Apr 17  2010 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2010 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2010 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2010


brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  2010 brtools
```

Procédure d'installation

1. Installez SAP R/3 BRTOOLS sur le système d'application.
2. Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :
   - `Agent HP StorageWorks P9000 XP`
   - `Intégration SAP R/3`
   - `Agent de disque`

REMARQUE :

Vous devez uniquement installer le composant `Intégration SAP R/3` sur le système de sauvegarde si vous envisagez d'exécuter des sessions ZDB compatibles SAP impliquant le démarrage de BRBACKUP sur ce système.

Sur les systèmes Windows, les composants logiciels de Data Protector doivent être installés avec le compte administrateur SAP R/3, et ce compte doit être inclus dans le groupe local `ORA_DBA` ou `ORA_SID_DBA` sur le système où l'instance SAP R/3 est exécutée.

Intégration de HP StorageWorks P9000 XP Disk Array Family avec Microsoft Exchange Server

Condition préalable

La base de données Microsoft Exchange Server doit être installée sur le système d'application, au niveau des volumes HP StorageWorks P9000 XP Disk Array Family (LDEV) mis en miroir sur le système de sauvegarde. La mise en miroir peut concerner HP BC P9000 XP ou HP CA P9000 XP 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 P9000 XP` – sur le système d'application et le système de sauvegarde
- `Intégration MS Exchange` – sur le système d'application uniquement

Intégration de HP StorageWorks P9000 XP Disk Array Family avec Microsoft SQL Server

Conditions préalables

Microsoft SQL Server doit être installé sur le système d'application. Les bases de données utilisateur *doivent* se trouver sur les volumes source 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 P9000 XP`
- `Intégration MS SQL`

Intégration HP StorageWorks P4000 SAN Solutions

Pour intégrer HP StorageWorks P4000 SAN Solutions avec Data Protector, installez les composants logiciels Data Protector suivants sur les systèmes d'application et de sauvegarde :

- `Intégration MS Volume Shadow Copy`
- `Agent HP StorageWorks P4000`

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)

  Avant d'installer à distance l'`Agent EMC Symmetrix`, installez les deux composants EMC suivants :

- EMC Solution Enabler
- Microcode et licence EMC Symmetrix TimeFinder ou EMC Symmetrix Remote Data Facility (SRDF)

- `Agent général de support`

  Installez le composant `Agent général de support` sur le système de sauvegarde pour sauvegarder les données en bloc. Installez-le sur le système d'application pour sauvegarder les journaux d'archive ou pour restaurer le système.

- `Agent de disque`

  Installez le composant `Agent de disque` sur les systèmes d'application et de sauvegarde pour exécuter des sauvegardes ZDB d'image disque et de système de fichiers. Les clients sans Agent de disque ne sont pas répertoriés dans les listes déroulantes `Système d'application` et `Système de sauvegarde` lors de la création d'une spécification de sauvegarde ZDB.

Installation sur un cluster

Vous pouvez installer l'intégration EMC Symmetrix dans un environnement de cluster. Pour connaître les configurations de clusters prises en charge et la configuration requise pour l'installation, reportez-vous au *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Intégration à d'autres applications

Si vous souhaitez installer l'intégration EMC Symmetrix avec une application de base de données, installez le composant Data Protector spécifique à l'intégration de cette application sur les systèmes d'application et de sauvegarde, et effectuez les tâches spécifiques à cette intégration. Vous pouvez installer l'intégration EMC Symmetrix avec Oracle et SAP R/3.

Intégration EMC Symmetrix avec Oracle

Configuration système requise

- Les logiciels suivants doivent être installés sur le système d'application :
  - Oracle Enterprise Server (RDBMS) ;
  - Services Oracle Net ;
  - SQL*Plus.

- Les fichiers de la base de données Oracle utilisés par le système d'application doivent être installés sur des périphériques EMC Symmetrix qui sont mis en miroir sur le système de sauvegarde.

  La base de données peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers. Les fichiers Oracle suivants doivent être mis en miroir :

  - fichiers de données ;
  - fichier de contrôle ;
  - fichiers journaux de rétablissement en ligne.

  Les fichiers journaux de rétablissement archivés doivent résider sur des disques qui ne sont pas en miroir.

Procédure d'installation

Procédez aux tâches d'installation suivantes :

1. Installez la base de données du catalogue de récupération Oracle. De préférence, installez-la sur un autre système, sur des disques qui ne sont pas en miroir. Laissez le catalogue de récupération non enregistré. Pour plus d'informations sur l'installation de la base de données, reportez-vous à la documentation Oracle.

2. Installez les composants logiciels Data Protector suivants :
   - `Agent EMC Symmetrix` – sur le système d'application et le système de sauvegarde
   - `Intégration Oracle` – sur le système d'application et le système de sauvegarde

REMARQUE :

- Le composant `Intégration Oracle` Data Protector sur le système de sauvegarde n'est nécessaire que pour la méthode de jeu de sauvegarde ZDB. Il n'est pas nécessaire pour la méthode proxy-copy ZDB.
- Dans un environnement de cluster RAC, plusieurs instances Oracle accèdent à la base de données d'application Oracle. Par conséquent, installez les composants `Intégration Oracle` et `Agent EMC Symmetrix` Data Protector sur tous les systèmes sur lesquels s'exécutent les instances Oracle.
- Si vous avez installé la base de données du catalogue de récupération Oracle sur un autre système, il n'est pas nécessaire d'y installer des composants logiciels Data Protector.

Intégration EMC Symmetrix avec SAP R/3

Configuration système requise

- Les logiciels Oracle suivants doivent être installés sur le système d'application :
  - Oracle Enterprise Server (RDBMS) ;
  - logiciel Oracle Net8 ;
  - SQL*Plus.
- Si vous envisagez d'exécuter des sessions ZDB compatibles SAP (BRBACKUP démarré sur le système de sauvegarde et non sur le système d'application), le système de sauvegarde doit être configuré. Pour plus de détails, reportez-vous au guide de la base de données SAP pour Oracle (sauvegarde split mirror, configuration du logiciel).
- La base de données du système d'application peut être installée sur des images disque, des volumes logiques ou des systèmes de fichiers.
  - Les fichiers de données Oracle *doivent* résider sur une baie de disques.

- Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas nécessairement résider sur une baie de disques. En revanche, pour les sessions ZDB *en ligne* compatibles SAP, les fichiers de contrôle doivent résider sur une baie de disques.
- Pour la *sauvegarde hors ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* résider sur une baie de disques.
- Les fichiers journaux de rétablissement archivés ne doivent pas nécessairement résider sur une baie de disques.

REMARQUE :

Si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez les liens également sur le système de sauvegarde.

UNIX seulement : Si la base de données Oracle est installée sur des partitions brutes (image disque ou volumes logiques bruts), vérifiez que les noms de volume/groupe de disques sont identiques sur le système d'application et le système de sauvegarde.

- Sous UNIX, vérifiez que les utilisateurs suivants sont définis sur le système d'application :
  - `ora`ORACLE_SID dans le groupe principal `dba`
  - ORACLE_SID`adm` dans le groupe UNIX `sapsys`
- Le logiciel SAP R/3 doit être correctement installé sur le système d'application.

  Les répertoires standard suivants doivent être installés sur le système d'application après l'installation de SAP R/3 :

REMARQUE :

L'emplacement des répertoires dépend des variables d'environnement. Reportez-vous à la documentation SAP R/3 pour plus d'informations.

  - ORACLE_HOME`/dbs` - les profils Oracle et SAP R/3
  - ORACLE_HOME`/bin` - les fichiers binaires Oracle
  - SAPDATA_HOME`/sapbackup` - le répertoire SAPBACKUP contenant les fichiers journaux BRBACKUP
  - SAPDATA_HOME`/sapbackup` - le répertoire SAPARCH contenant les fichiers journaux BRARCHIVE
  - SAPDATA_HOME`/sapreorg`

- SAPDATA_HOME/sapcheck
- SAPDATA_HOME/saptrace
- /usr/sap/ORACLE_SID/SYS/exe/run

REMARQUE :

Si vous envisagez d'effectuer une restauration instantanée, vérifiez que les répertoires sapbackup, saparch et sapreorg figurent sur d'autres volumes source que les fichiers de données Oracle.

Si les six derniers répertoires ne sont pas aux emplacements indiqués ci-dessus, créez les liens appropriés vers eux.

Le propriétaire du répertoire /usr/sap/ORACLE_SID/SYS/exe/run doit être l'utilisateur UNIX ora*ORACLE_SID*. Le propriétaire des fichiers SAP R/3 doit être l'utilisateur UNIX ora*ORACLE_SID* et le groupe UNIX dba avec le bit setuid à 1 (chmod 4755 ...). L'exception est le fichier BRRESTORE, dont le propriétaire doit être l'utilisateur UNIX *ORACLE_SID*adm.

Exemple

Si *ORACLE_SID* est PRO, les droits à l'intérieur du répertoire /usr/sap/PRO/SYS/exe/run doivent ressembler à ce qui suit :

```
-rwsr-xr-x   1 orapro dba 4598276 Apr 17  2010 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2010 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2010 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2010 brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  2010 brtools
```

Procédure d'installation

1. Installez SAP R/3 BRTOOLS sur le système d'application.
2. Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :
   - Agent EMC Symmetrix
   - Intégration SAP R/3
   - Agent de disque

REMARQUE :

Il n'est pas nécessaire d'installer `Intégration SAP R/3` sur le système de sauvegarde si vous envisagez d'exécuter des sessions ZDB compatibles SAP lors desquelles BRBACKUP est démarré sur ce système.

Intégration d'EMC Symmetrix avec Microsoft SQL Server

Conditions préalables

Microsoft SQL Server doit être installé sur le système d'application. Les bases de données utilisateur *doivent* se trouver sur les volumes source de la baie de disques, tandis que les bases de données système peuvent être installées n'importe où. Cependant, si les bases de données système sont elles aussi installées sur la baie de disques, elles *doivent* l'être sur des volumes source *différents* de ceux des bases de données utilisateur.

Procédure d'installation

Installez les composants logiciels Data Protector suivants sur le système d'application et le système de sauvegarde :

- `Agent EMC Symmetrix`
- `Intégration MS SQL`

Clients d'auto-migration VLS

La fonction de copie de supports de Data Protector vous permet de copier des supports après une sauvegarde. L'intégration avec HP StorageWorks Virtual Library System (VLS) enrichit cette fonctionnalité en proposant une solution qui associe les fonctions de copie internes de VLS aux fonctions de gestion et de suivi des supports de Data Protector.

Pour intégrer Data Protector avec l'auto-migration VLS pour réaliser des copies de supports intelligentes, installez les composants logiciels d'`auto-migration VLS` Data Protector.

Configuration requise

Effectuez les opérations suivantes :

1. Configurez le stockage virtuel VLS selon la configuration requise en utilisant Command View VLS. Pour plus d'informations, voir la documentation de VLS.
2. Connectez une ou plusieurs bibliothèques physiques au VLS.
3. Importez le client VLS dans la cellule Data Protector.

Installation de l'interface utilisateur localisée de Data Protector

Data Protector 6.20 dispose d'une interface utilisateur graphique localisée de Data Protector sur les systèmes Windows et UNIX. Elle est constituée de l'interface utilisateur graphique et de l'interface de ligne de commande localisées de Data Protector. De la documentation localisée (guides et aide en ligne) est également fournie. Pour plus d'informations sur les parties localisées ou non du jeu de documentation Data Protector, consultez les *Références, notes de publication et annonces produits HP Data Protector*.

REMARQUE :

Par défaut, lors de l'installation de Data Protector, le support de toutes les langues prises en charge est installé et l'interface utilisateur localisée de Data Protector est lancée conformément à l'environnement local défini au niveau du système.

Dépannage

Si la version anglaise de l'interface utilisateur d'origine de Data Protector démarre après que vous avez installé un support de langue différent, effectuez les vérifications suivantes :

1. Assurez-vous que les fichiers suivants existent :

   Pour le support de langue français :

   - Sous Windows : `répertoire_Data_Protector\bin\OmniFra.dll`
   - Sous HP-UX : `/opt/omni/lib/nls/fr.iso88591/omni.cat`
   - Sous Solaris : `/opt/omni/lib/nls/fr.ISO8859-1/omni.cat`

   Pour le support de langue japonais :

   - Sous Windows : `répertoire_Data_Protector\bin\OmniJpn.dll`
   - Sous HP-UX : `/opt/omni/lib/nls/ja.eucJP/omni.cat` et `/opt/omni/lib/nls/ja.SJIS/omni.cat`
   - Sous Solaris : `/opt/omni/lib/nls/ja.eucJP/omni.cat` et `/opt/omni/lib/nls/ja.PCK/omni.cat`

   Pour le support de langue chinois simplifié :

   - Sous Windows : `répertoire_Data_Protector\bin\OmniChs.dll`
   - Sous HP-UX : `/opt/omni/lib/nls/zh_CN.gb18030/omni.cat` et `/opt/omni/lib/nls/zh_CN.gb18030/omni.cat`
   - Sous Solaris : `/opt/omni/lib/nls/zh_CN.GB18030/omni.cat` et `/opt/omni/lib/nls/zh_CN.GB18030/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 japonais ; `zh_CN.GB18030` pour le chinois simplifié et `fr_FR.iso88591` pour le 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 la documentation Data Protector localisée

Installation de la documentation Data Protector localisée sur les systèmes Windows

Installation en local

Pour installer la documentation localisée de Data Protector en local sur des systèmes Windows, sélectionnez le composant approprié dans la page **Installation personnalisée** de l'assistant **d'installation**, comme indiqué à la Figure 23 à la page 198.

Pour connaître la procédure d'installation locale, reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector” à la page 44.

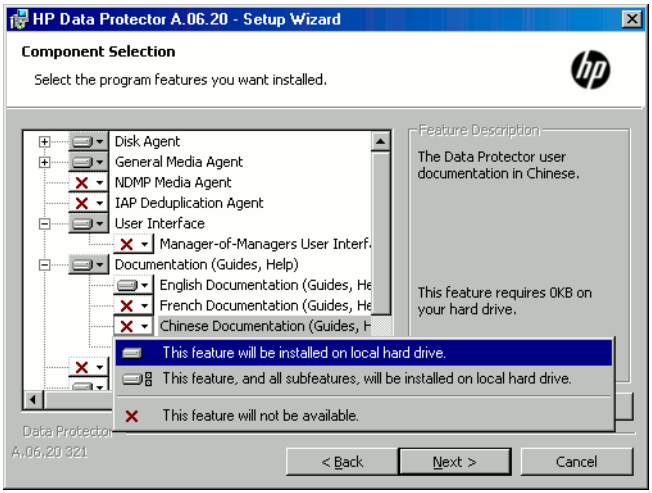


Figure 23 Sélection de la documentation localisée lors de l'installation

Installation à distance

Lors de la distribution à distance de la documentation localisée de Data Protector à l'aide du Serveur d'installation, sélectionnez le composant approprié dans la page **Sélection des composants** de l'assistant **Ajouter composants**, comme indiqué à la Figure 24 à la page 199.

Pour connaître la procédure d'ajout à distance de composants logiciels Data Protector à des clients, reportez-vous à la section “Installation distante de clients Data Protector” à la page 83.

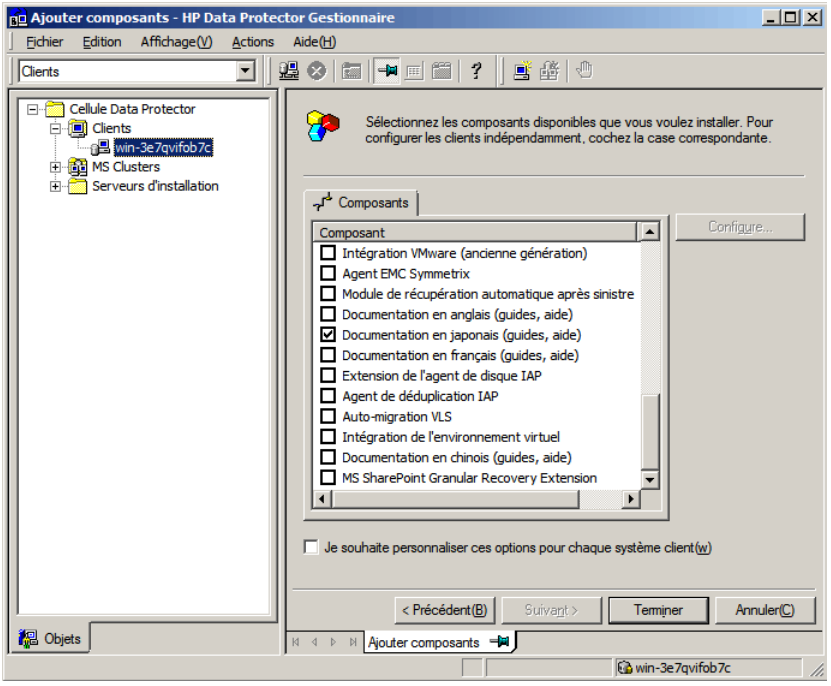


Figure 24 Installation à distance de la documentation localisée

Installation de la documentation Data Protector localisée sur les systèmes UNIX

Installation en local

Vous pouvez installer en local la documentation en français, japonais ou chinois simplifié uniquement sur un client Data Protector à l'aide de la commande `omnisetup.shcommande omnisetup.shinstallationcommandesomnisetup.sh`. Spécifiez le composant logiciel `fra_ls`, `jpn_ls` ou `chs_ls` en fonction du support de langue souhaité. Pour connaître la procédure détaillée, reportez-vous à la section “Installation en local de clients UNIX et Mac OS X” à la page 151.

Si vous utilisez l'utilitaire `swinstall`, `pkgadd` ou `rpm` pour installer le Gestionnaire de cellule ou le Serveur d'installation de Data Protector, vous pouvez uniquement installer la documentation en anglais. Si vous voulez 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 les packs de langues supplémentaires à distance.

Installation distante

Lors de la distribution à distance de la documentation localisée de Data Protector à l'aide du Serveur d'installation, sélectionnez le composant approprié dans la page **Sélection des composants** de l'assistant **Ajouter composants**, comme indiqué à la Figure 24 à la page 199.

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 83.

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 44.

Limites

Lorsque vous examinez la licence de l'Edition serveur unique, tenez compte des limites suivantes :

Limites de l'Edition serveur unique pour Windows

- L'Edition serveur unique prend en charge les sauvegardes vers un seul périphérique à la fois, lequel est connecté à un seul Gestionnaire de cellule.
- Elle ne prend en charge qu'un changeur automatique DDS à 10 emplacements.
- Elle ne prend en charge ni les clients, ni les serveurs UNIX (et HP-UX). Si vous essayez d'effectuer une sauvegarde sur une machine UNIX, la session est abandonnée.
- Si une cellule contient un Gestionnaire de cellule Windows, vous ne pouvez sauvegarder que des clients Windows. L'Edition serveur unique ne prend pas en charge la sauvegarde vers les clients Novell NetWare.

- L'ajout de produits d'extension n'est pas pris en charge par l'Edition serveur unique.
- La gestion de clusters n'est pas prise en charge par l'Edition serveur unique.
- La récupération après sinistre n'est pas prise en charge.

Le nombre de clients Windows n'est pas limité.

Pour connaître les périphériques pris en charge, reportez-vous aux Références, notes de publication et annonces produits HP Data Protector.

Limites de l'Edition serveur unique pour HP-UX et Solaris

- L'Edition serveur unique prend en charge les sauvegardes vers un seul périphérique à la fois, lequel est connecté à un seul Gestionnaire de cellule.
- Elle ne prend en charge qu'un changeur automatique DDS à 10 emplacements.
- Sur un Gestionnaire de cellule UNIX, vous ne pouvez pas sauvegarder des serveurs, mais seulement des clients UNIX, des clients Windows, des clients Solaris et des clients Novell NetWare.
- L'ajout de produits d'extension n'est pas pris en charge par l'Edition serveur unique.
- La gestion de clusters n'est pas prise en charge par l'Edition serveur unique.

Le nombre de clients (UNIX, Windows) n'est pas limité.

Pour connaître les périphériques pris en charge, reportez-vous aux Références, notes de publication et annonces produits HP Data Protector.

Installation d'un mot de passe

Pour obtenir des instructions détaillées sur l'installation d'un mot de passe sur le Gestionnaire de cellule, reportez-vous à la section “Mots de passe Data Protector” à la page 347.

Installation des Rapports Web de Data Protector

Le composant Rapports Web de Data Protector est installé par défaut avec d'autres composants Data Protector et à ce titre, vous pouvez l'utiliser en local à partir de votre système.

Vous pouvez également l'installer sur un serveur Web et ainsi le rendre disponible sur les autres systèmes, sur lesquels l'installation des composants logiciels Data Protector n'est pas obligatoire.

Configuration système requise

Pour utiliser la génération de rapports Web de Data Protector sur votre système, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector* pour connaître la configuration requise et les limites.

Installation

Procédez comme suit pour installer le composant Rapports Web Data Protector sur un serveur Web :

1. Copiez les fichiers de rapport Java Data Protector suivants sur le serveur. Il n'est pas nécessaire que le serveur soit un client Data Protector.
   - Sur les systèmes Windows disposant de l'interface utilisateur Data Protector, les fichiers se trouvent dans le répertoire suivant :

     `répertoire_Data_Protector\java\bin`
   - Sur un système UNIX disposant de l'interface utilisateur Data Protector, les fichiers se trouvent dans le répertoire suivant :

     `/opt/omni/java/bin`
2. Ouvrez le fichier `WebReporting.html` dans votre navigateur pour accéder aux Rapports Web de Data Protector.

   Vous devez rendre le fichier disponible aux utilisateurs des Rapports Web sous forme d'URL complète. Par exemple, vous pouvez placer un lien vers ce fichier à partir de votre site Intranet.

CONSEIL :

Aucun mot de passe n'est requis par défaut pour utiliser les Rapports Web Data Protector. Vous pouvez cependant en indiquer un et restreindre ainsi l'accès aux Rapports Web. Pour connaître la procédure à suivre, reportez-vous à l'index de l'aide en ligne (rubrique "rapports Web, restriction d'accès").

Etape suivante

Une fois l'installation terminée, reportez-vous à l'index de l'aide en ligne (rubrique "interface de génération de rapports Web, configuration de notifications") pour plus d'informations sur les questions de configuration et la création de rapports personnalisés.

Installation de Data Protector sur MC/ServiceGuard

Data Protector prend en charge MC/ServiceGuard (MC/SG) pour HP-UX et Linux. Pour obtenir des informations détaillées sur les versions de systèmes d'exploitation prises en charge, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

Si votre Gestionnaire de cellule doit être compatible cluster, notez que l'adresse IP du serveur virtuel doit être utilisée pour les licences.

Installation d'un Gestionnaire de cellule compatible cluster

Configuration système requise

Avant d'installer un Gestionnaire de cellule Data Protector sur MC/ServiceGuard, vérifiez les éléments suivants :

- Décidez quels systèmes seront les Gestionnaires de cellule principal et secondaire. Ils doivent tous être équipés de MC/ServiceGuard et configurés en tant que membres du cluster.
- 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 44.

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 Serveur d'installation sur des noeuds de cluster

Vous pouvez installer le Serveur d'installation sur un noeud MC/ServiceGuard secondaire et l'utiliser pour une installation à distance. Voir “Installation des Serveurs d'installation pour UNIX” à la page 64.

Installation de clients compatibles 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 99 et “Installation de clients Linux” à la page 110.

Etape suivante

Lorsque vous avez terminé l'installation, vous devez importer le serveur virtuel (nom d'hôte spécifié dans le package de clusters) dans la cellule Data Protector. Reportez-vous à la section “Importation d'un client compatible cluster dans une cellule” à la page 225.

Reportez-vous à *l'index de l'aide en ligne (rubrique "configuration")* pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration de Data Protector.

Installation de Data Protector sur Microsoft Cluster Server

Pour connaître les systèmes d'exploitation pris en charge pour l'intégration de Microsoft Cluster Server, consultez les dernières matrices de support à l'adresse http://www.hp.com/support/manuals.

REMARQUE :

Si votre Gestionnaire de cellule doit être compatible cluster, l'adresse IP du serveur virtuel du Gestionnaire de cellule doit être utilisée pour les licences.

Installation d'un Gestionnaire de cellule compatible cluster

Configuration système requise

Avant d'installer le Gestionnaire de cellule Data Protector compatible cluster, les conditions préalables suivantes doivent être remplies :

- La fonctionnalité de cluster doit être installée sur tous les noeuds cluster. Par exemple, vous devez pouvoir déplacer des groupes d'un noeud à l'autre autant de fois que cela est nécessaire, et ce sans aucun problème de disque partagé.
- Veillez à ce qu'il n'existe pas sur le cluster de ressources avec les noms suivants :

  `OBVS_MCRS`, `OBVS_VELOCIS`, `OmniBack_Share`

  Data Protector utilise ces noms pour le serveur virtuel Data Protector. Si ce type de ressource existe, supprimez-les ou renommez-les.

  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.

- Un groupe au moins du cluster doit disposer d'une ressource de cluster de fichiers définie. Data Protector installera certains de ses fichiers de données dans un dossier particulier de cette ressource de cluster de fichiers.

  Sous Windows Server 2008, les fichiers de données sont installés dans le dossier de la ressource *`Serveur de fichiers`* sélectionné par l'utilisateur lors de l'installation.

  Sur les autres systèmes Windows, les fichiers de données sont installés dans le dossier de la ressource *`Partage de fichiers`* défini lors de la création de la ressource de cluster de fichiers.

  Pour plus d'informations sur la définition d'une ressource de cluster de fichiers, consultez la documentation propre aux clusters. Notez que le nom de partage de fichiers de cette ressource ne peut pas être `OmniBack`.

- Si le serveur virtuel n'existe pas dans le même groupe que la ressource de cluster de fichiers, créez un nouveau serveur virtuel en utilisant une adresse IP libre enregistrée et associez-lui un nom de réseau.
- La ressource de cluster de fichiers dans laquelle Data Protector sera installé doit disposer d'une `adresse IP`, d'un `nom de réseau` et d'un ensemble de `disques physiques` parmi ses dépendances. Cela permet l'exécution du

groupe de clusters Data Protector sur n'importe quel nœud, indépendamment de tout autre groupe.

- Assurez-vous que seul l'administrateur de clusters a accès au dossier partagé de la ressource de cluster de fichiers et qu'il bénéficie d'un accès complet.
- Data Protector est installé au même endroit (lecteur et chemin d'accès) sur tous les noeuds cluster. Assurez-vous que ces emplacements sont libres.
- Si vous lancez l'installation compatible cluster de Gestionnaire de cellule à partir d'un partage réseau, vous devez avoir accès à ce partage depuis tous les noeuds de cluster.
- Vérifiez qu'aucune autre installation basée sur Microsoft Installer n'est en cours d'exécution sur d'autres nœuds du cluster.
- Chaque système (noeud) du cluster doit être en cours d'exécution.
- Pour permettre l'installation du Gestionnaire de cellule Data Protector compatible cluster sur un cluster de server sur lequel Microsoft Cluster Service (MSCS) fonctionne sous Windows Server 2008, suivez la procédure fournie à la section "Préparation d'un cluster de serveur Microsoft sous Windows Server 2008 à l'installation de Data Protector" à la page 417.

Eléments à prendre en considération

- L'installation doit être démarrée sous le compte de service cluster sur le système (noeud) sur lequel la ressource de cluster de fichiers est active, afin de permettre un accès direct à son dossier partagé. Vous pouvez déterminer le propriétaire de la ressource (le système sur lequel la ressource est active) à l'aide de l'administrateur de clusters.
- Pour une installation et une configuration correctes du Gestionnaire de cellule Data Protector compatible cluster, un compte de domaine avec les droits d'utilisateur suivants doit être fourni pendant l'installation :
  - Droits d'administrateur sur le système 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

IMPORTANT :

Pour installer Microsoft Cluster Server, vous devez disposer d'un compte bénéficiant de droits d'administrateur sur tous les systèmes de clusters (noeuds). Vous devez également utiliser ce compte pour installer Data Protector. Si vous ignorez ces points, les services Data Protector s'exécutent en mode ordinaire au lieu du mode compatible cluster.

Procédure d'installation locale

Vous devez installer en local le Gestionnaire de cellule Data Protector compatible cluster à partir du DVD-ROM. Effectuez les opérations suivantes :

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

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

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

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

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

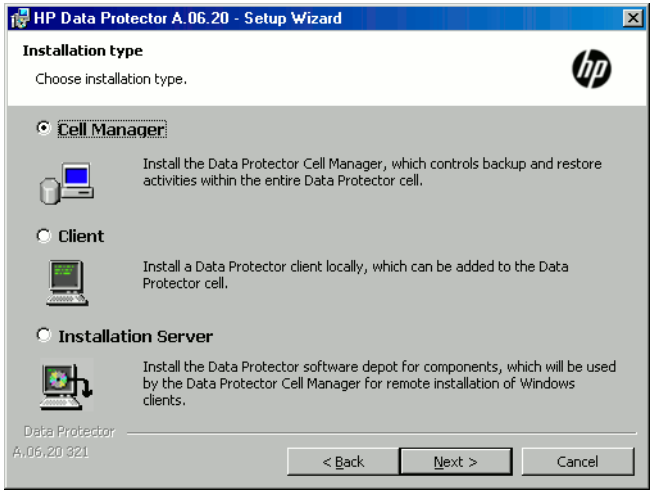


Figure 25 Sélection du type d'installation

5. Le processus d'installation détecte automatiquement qu'il fonctionne dans un environnement de clusters. Sélectionnez **Install cluster-aware Cell Manager (Installation du Gestionnaire de cellule compatible cluster)** pour activer la configuration d'un cluster.

   Sélectionnez le groupe de clusters, le nom d'hôte virtuel et la ressource de cluster de fichiers sur laquelle résideront les fichiers partagés et la base de données de Data Protector.

REMARQUE :

Si vous sélectionnez **Install Gestionnaire de cellule on this node only (Installer le Gestionnaire de cellule sur ce noeud uniquement)**, le Gestionnaire de cellule *ne sera pas* compatible cluster. Reportez-vous à la section “Installation d'un Gestionnaire de cellule Windows” à la page 55.

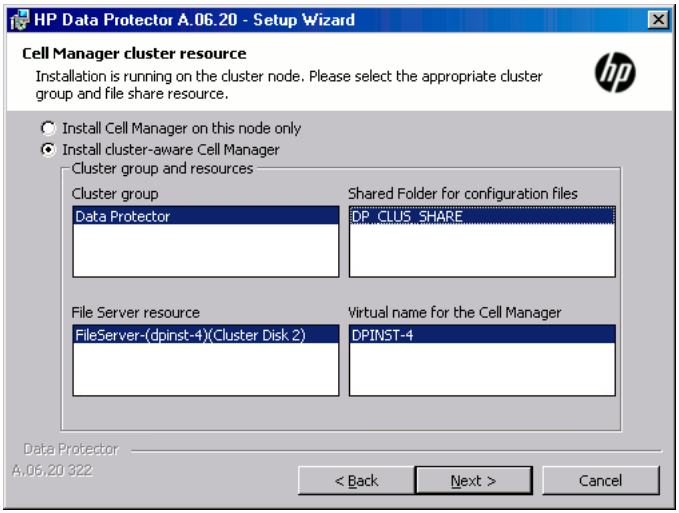


Figure 26 Sélection de la ressource de cluster sous Windows Server 2008

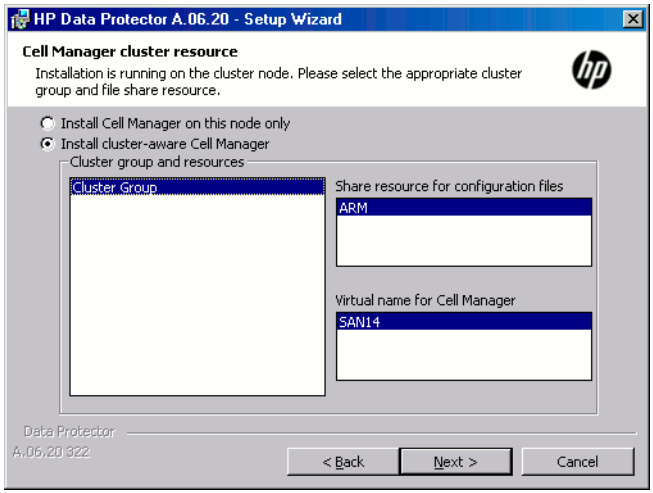


Figure 27 Sélection de la ressource de cluster sur les autres systèmes Windows

6. Saisissez le nom d'utilisateur et le mot de passe correspondant au compte qui sera utilisé pour lancer les services Data Protector.

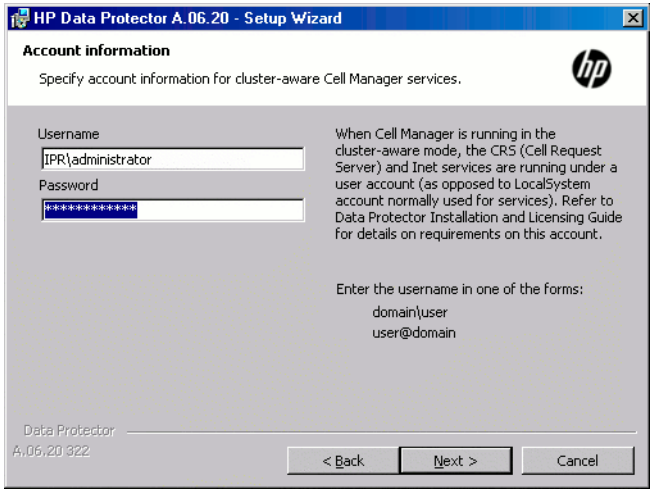


Figure 28 Saisie des informations relatives au compte

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

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

8. Dans la fenêtre Sélection des composants, sélectionnez les composants que vous souhaitez installer sur tous les nœuds cluster et les serveurs virtuels cluster. Cliquez sur **Suivant**.

   Les fichiers du composant Prise en charge du cluster MS sont installés automatiquement.

   Les composants sélectionnés seront installés sur tous les noeuds du cluster.

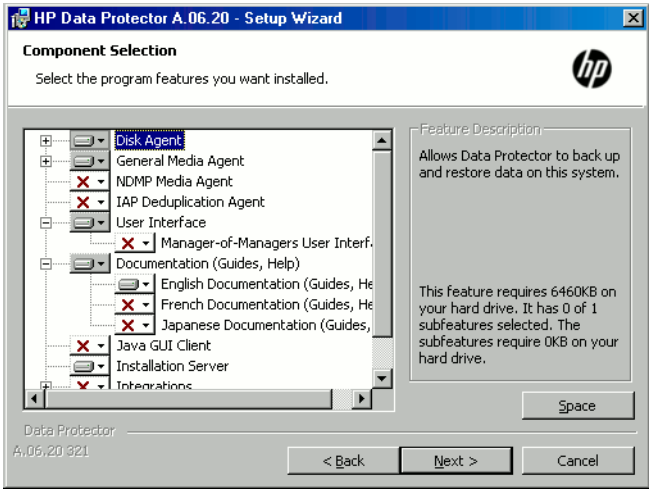


Figure 29 Page de sélection des composants

9. *Si Data Protector détecte le pare-feu Windows sur votre système*, la page Configuration du pare-feu Windows apparaît. Le programme d'installation de Data Protector y enregistre 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**.

10. La liste des composants sélectionnés s'affiche. Cliquez sur **Installer**.

11. La page Installation setup (Configuration de l'installation) s'affiche. Cliquez sur **Suivant**.

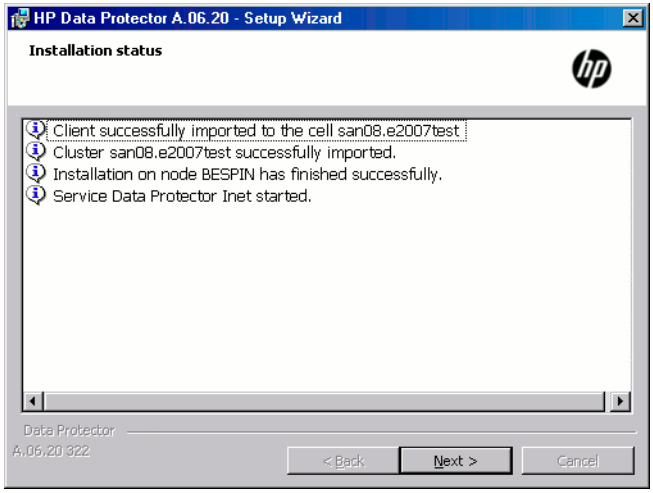


Figure 30 Page d'état de l'installation

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

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

    Sur les systèmes d'exploitation autres que Windows Server 2003 x64 et Windows Server 2008 x64, pour installer ou mettre à niveau l'utilitaire HP AutoPass, sélectionnez l'option **Start AutoPass installation (Démarrer l'installation d'AutoPass)** ou **Upgrade AutoPass installation (Mettre à niveau l'installation d'AutoPass)**.

    Il n'est *pas* recommandé d'installer l'utilitaire HP AutoPass sur un cluster de serveur Microsoft, car il ne serait installé que sur un seul noeud et non sur tous. Toutefois, si vous installez AutoPass, vous devez désinstaller Data Protector du noeud sur lequel il était installé, une fois que vous décidez de supprimer Data Protector du système.

    HP AutoPass n'est pas installé sur les systèmes d'exploitation Windows Server 2003 x64 et Windows Server 2008 x64.

13. Cliquez sur **Terminer** pour terminer l'installation.

Vérification de l'installation

Une fois l'installation terminée, vous pouvez vous assurer que le logiciel Data Protector a été installé correctement. Pour ce faire, procédez comme suit :

1. Vérifiez si le compte de service cluster est affecté au service `Inet` Data Protector sur chaque nœud du cluster. Vérifiez que le même utilisateur est également ajouté au groupe d'utilisateurs Admin de Data Protector. Le type de compte de connexion défini doit être `Ce compte` comme illustré dans la Figure 31 à la page 212.

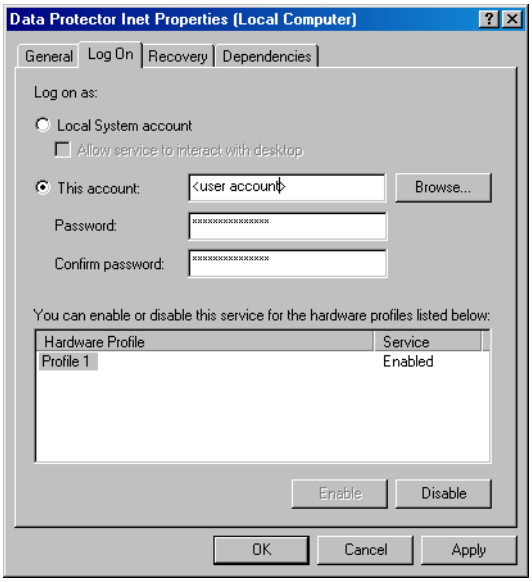


Figure 31 Compte utilisateur Data Protector

2. Basculez vers le répertoire `répertoire_Data_Protector\bin` et exécutez la commande suivante :

   `omnirsh` *`hôte`* `INFO_CLUS`

   où *`hôte`* est le nom du serveur virtuel cluster (sensible à la casse). Le résultat doit contenir la liste des noms des systèmes se trouvant dans le cluster et le nom du serveur virtuel. Si `0 "NONE"` est affiché, Data Protector n'est pas installé en mode compatible cluster.

3. Lancez l'interface utilisateur graphique de Data Protector, sélectionnez le contexte **Clients**, puis cliquez sur **MS Clusters.** Les systèmes récemment installés doivent apparaître dans la zone de résultats.

Services Inet et CRS de Data Protector

Si nécessaire, modifiez les comptes sous lesquels s'exécutent les services `Inet` et `CRS` de Data Protector.

Installation de clients compatibles cluster

Configuration système requise

Avant d'installer un client Data Protector compatible cluster, les conditions préalables suivantes doivent être remplies :

- La fonctionnalité de cluster doit être installée sur tous les noeuds cluster. Par exemple, vous devez pouvoir déplacer des groupes d'un noeud 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.
- Pour permettre l'installation du client Data Protector compatible cluster sur un cluster de server sur lequel Microsoft Cluster Service (MSCS) fonctionne sous Windows Server 2008, suivez la procédure fournie à la section “Préparation d'un cluster de serveur Microsoft sous Windows Server 2008 à l'installation de Data Protector” à la page 417.

Procédure d'installation locale

Les clients Data Protector compatibles cluster doivent être installés localement, à partir du DVD-ROM, sur chaque nœud du cluster. Les nœuds cluster (clients cluster Data Protector) sont importés vers la cellule spécifiée lors du processus d'installation. Vous devez ensuite importer le nom du serveur virtuel.

Les droits administrateur de clusters sont requis pour effectuer l'installation. Hormis cette exigence, la configuration d'un client cluster est la même que celle d'un client Windows classique. Les fichiers du composant Prise en charge du cluster MS sont installés automatiquement.

Reportez-vous à la section “Installation de clients Windows” à la page 92 pour plus d'informations sur l'installation en local d'un système client Windows Data Protector.

Le processus d'installation de Data Protector signale qu'un cluster a été détecté. Sélectionnez **Installer le client en mode compatible cluster**.

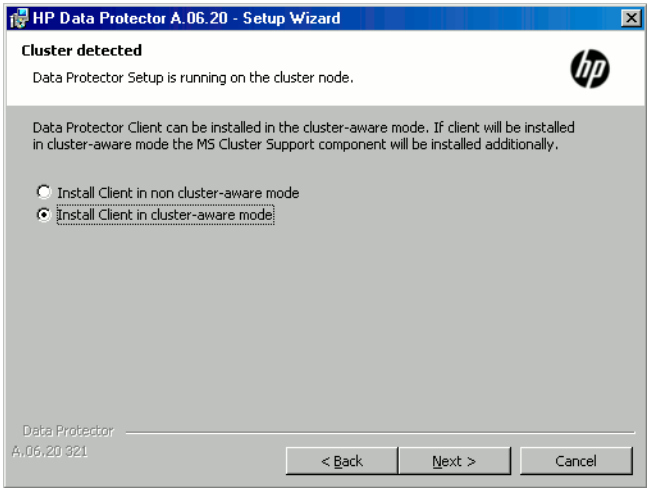


Figure 32 Sélection du mode d'installation compatible cluster

Si vous installez l'intégration Data Protector Oracle, la procédure de configuration doit être effectuée sur tous les nœuds du cluster, ainsi que sur le serveur virtuel hébergeant le groupe de ressources Oracle.

REMARQUE :

Vous pouvez importer un client compatible cluster dans la cellule Data Protector qui est gérée par le Gestionnaire de cellule standard ou par le Gestionnaire de cellule compatible cluster.

Vérification de l'installation

Une fois l'installation terminée, vous pouvez vous assurer que le logiciel Data Protector a été installé correctement. Pour ce faire, procédez comme suit :

1. Vérifiez si le compte de service cluster est affecté au service `Inet` Data Protector sur chaque nœud du cluster. Vérifiez que le même utilisateur est également ajouté au groupe d'utilisateurs `Admin` de Data Protector. Le type de compte de connexion défini doit être **Ce compte** comme illustré dans la Figure 33 à la page 215.

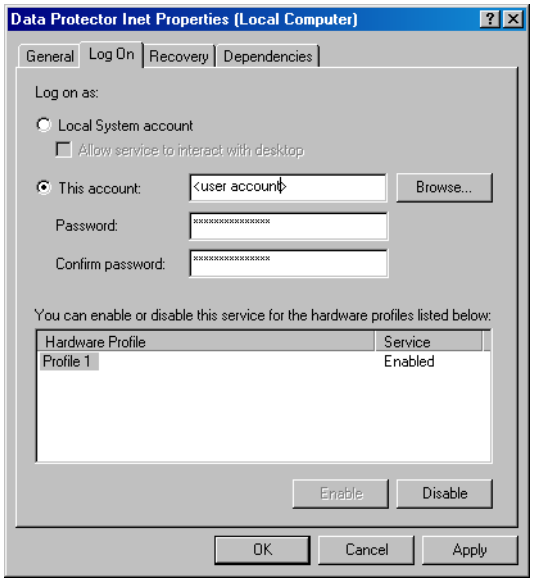


Figure 33 Compte utilisateur Data Protector

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 Server avec Veritas Volume Manager” à la page 420.

Etape suivante

Lorsque vous avez terminé l'installation, vous devez importer le nom d'hôte du serveur virtuel (application compatible cluster) dans la cellule Data Protector. Reportez-vous à la section “Importation d'un client compatible cluster dans une cellule” à la page 225.

Reportez-vous à l'index de l'aide en ligne (rubrique "configuration") pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration Data Protector.

Modification des comptes Inet et CRS

Si nécessaire, modifiez les comptes sous lesquels s'exécutent les services `Inet` et `CRS` de Data Protector.

Installation de clients Data Protector sur un cluster Veritas

Il est possible d'installer les clients Data Protector sur des nœuds cluster Veritas, à l'aide d'un Gestionnaire de cellule extérieur au cluster. Si vous utilisez cette configuration, la sauvegarde des disques locaux est prise en charge.

Notez que si vous souhaitez sauvegarder des disques partagés ou des applications compatibles cluster, il faut utiliser l'adresse IP du serveur virtuel pour les licences.

IMPORTANT :

Pour Data Protector, les sauvegardes compatibles cluster avec basculement ne sont pas prises en charge.

Installation de clients compatibles cluster

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 103.

Etape suivante

Une fois l'installation terminée :

- Si vous souhaitez sauvegarder le serveur virtuel, vous devez l'importer dans la cellule.
- Si vous souhaitez sauvegarder les nœuds physiques, vous devez également les importer dans la cellule.

Reportez-vous à la section "Importation d'un client compatible cluster dans une cellule" à la page 225. Reportez-vous à l'index de l'aide en ligne (rubrique "configuration") pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration de Data Protector.

Installation de clients Data Protector sur un cluster Novell NetWare

Il est possible d'installer les clients Data Protector sur des nœuds cluster Novell NetWare Cluster Services, à l'aide d'un Gestionnaire de cellule extérieur au cluster. Si vous utilisez cette configuration, la sauvegarde des disques locaux, ainsi que la sauvegarde des pools de clusters partagés, sont prises en charge via le serveur virtuel. Pour connaître les systèmes d'exploitation pris en charge pour Microsoft Cluster Server, reportez-vous au document Références, notes de publication et annonces produits HP Data Protector.

Notez que si vous souhaitez sauvegarder des disques partagés ou des applications compatibles cluster, il faut utiliser l'adresse IP du serveur virtuel pour les licences.

IMPORTANT :

Les sauvegardes compatibles cluster avec basculement ne sont pas prises en charge. En cas de basculement, il faut redémarrer manuellement les sessions de sauvegarde ou de restauration.

Dans la mesure où les nœuds cluster contrôlent les périphériques, les périphériques de sauvegarde doivent être configurés sur les nœuds cluster et non sur le serveur virtuel.

Installation de clients compatibles cluster

Avant l'installation

Avant d'installer des clients Data Protector sur des nœuds cluster Novell NetWare Cluster Services, il est recommandé de modifier les scripts de déchargement pour *chaque* serveur virtuel présent dans le cluster, afin que l'adresse IP secondaire reste active pendant la migration du serveur virtuel vers un autre nœud. Vous pouvez modifier les scripts de déchargement à l'aide de l'utilitaire Console One de Novell ou de NetWare Remote Manager, conformément à la documentation Novell NetWare.

Exemple

Le script de déchargement par défaut pour chaque serveur virtuel est le suivant :

```
del secondary ipaddress 10.81.1.173
CLUSTER CVSBIND DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
NUDP DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
nss /pooldeactivate=FIRST /overridetype=question
```

Le script de déchargement modifié pour chaque serveur virtuel est le suivant :

```
nss /pooldeactivate=FIRST /overridetype=question
del secondary ipaddress 10.81.1.173
CLUSTER CVSBIND DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
NUDP DEL TREENW6_CLUSTER_FIRST_SERVER 10.81.1.173
```

Le script de déchargement modifié commence par démonter et désactiver tous les pools de clusters partagés sur le serveur virtuel ; alors seulement, il supprime l'adresse IP secondaire. Cela signifie que l'adresse IP secondaire reste active pendant la migration.

Pour activer le script de déchargement modifié, mettez le serveur virtuel hors ligne, puis de nouveau en ligne sur le nœud favori.

Modification du script smsrun.bas

Après avoir modifier le(s) script(s) de déchargement, vous devez modifier le script `smsrun.bas` afin d'inclure le chargement du module `TSA600.NLM` (ou `TSAFS.NLM` - selon le module que vous utilisez) avec le paramètre approprié désactivant la prise en charge du cluster. Pour plus d'informations, consultez la rubrique “Known Backup/Restore Issues for NetWare 6.x” (problèmes de sauvegarde/restauration connus pour NetWare 6.x) de la base de données Novell Support Knowledge.

Pour modifier le script `smsrun.bas`, procédez comme suit :

1. Modifiez la protection en écriture du script SYS:NSN/user/smsrun.bas en le faisant passer de `lecture seule` à `lecture/écriture`, puis ouvrez-le dans un éditeur standard de la console.
2. Modifiez la ligne `nlmArray = Array("SMDR", "TSA600", "TSAPROXY")` (ou `nlmArray = Array("SMDR", "TSAFS /NoCluster")`) dans la section `Sub Main()` en indiquant :
   - `nlmArray = Array("SMDR", "TSA600 /cluster=off", "TSAPROXY")` si TSA600 est installé.
   - `nlmArray = Array("SMDR", "TSAFS /NoCluster")` si TSAFS est installé.

   Enregistrez les modifications.
3. Sur la console du serveur de fichiers, tapez SMSSTOP.
4. Sur la console du serveur de fichiers, tapez SMSSTART.

Les volumes partagés du cluster sont désormais visibles pour le module TSA600.NLM(TSAFS.NLM).

Installation

La procédure est identique à celle utilisée pour l'installation standard locale de Data Protector sur un client Novell NetWare. Pour connaître la procédure détaillée, reportez-vous à la section "Installation en local de clients Novell NetWare" à la page 134.

Etape suivante

Une fois l'installation terminée :

- Si vous souhaitez sauvegarder les nœuds physiques, vous devez également les importer dans la cellule.
- Pour sauvegarder le serveur virtuel (volumes partagés du cluster), vous devez l'importer dans la cellule.

Reportez-vous à la section "Importation d'un client compatible cluster dans une cellule" à la page 225. Reportez-vous à l'index de l'aide en ligne (rubrique "configuration") pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration de Data Protector.

Installation de Data Protector sur un cluster IBM HACMP

Data Protector prend en charge IBM HACMP (High Availability Cluster Multi-Processing) pour AIX.

IMPORTANT :

Installez le composant Agent de disque Data Protector sur tous les noeuds du cluster.

Installation de clients compatibles cluster

Pour installer des composants Data Protector sur un noeud du cluster, utilisez la procédure d'installation standard de Data Protector sur des systèmes UNIX. Pour plus d'informations, reportez-vous aux sections “Installation en local de clients UNIX et Mac OS X” à la page 151 ou “Installation distante de clients Data Protector” à la page 83.

Etape suivante

Après l'installation, importez les nœuds du cluster et le serveur virtuel (adresse IP du package de l'environnement virtuel) dans la cellule Data Protector. Reportez-vous à la section “Importation d'un client compatible cluster dans une cellule” à la page 225.

Pour plus d'informations sur la configuration de périphériques de sauvegarde ou de pools de supports ou sur toute autre tâche de configuration de Data Protector, recherchez l'entrée suivante dans l'index de l'aide en ligne : configuration.

3 Gestion de l'installation

Dans ce chapitre

Ce chapitre décrit les procédures les plus utilisées pour modifier la configuration de votre environnement de sauvegarde. Les sections suivantes contiennent des informations relatives aux éléments suivants :

- Comment importer des clients dans une cellule à l'aide de l'interface utilisateur graphique. Reportez-vous à la section “Importation de clients dans une cellule ” à la page 222.
- Comment importer un Serveur d'installation dans une cellule à l'aide de l'interface utilisateur graphique. Reportez-vous à la section “Importation d'un serveur d'installation dans une cellule ” à la page 224.
- Comment importer des clusters/serveurs virtuels à l'aide de l'interface utilisateur graphique. Reportez-vous à la section “Importation d'un client compatible cluster dans une cellule” à la page 225.
- Comment exporter des clients à l'aide de l'interface utilisateur graphique. Reportez-vous à la section “Désinstallation du logiciel Data Protector” à la page 252.
- Comment garantir la sécurité à l'aide de l'interface utilisateur graphique. Reportez-vous à la section “A propos de la sécurité” à la page 231.
- Comment vérifier quels correctifs Data Protector sont installés. Reportez-vous à la section “Contrôle des correctifs Data Protector installés” à la page 250.
- Comment désinstaller le logiciel Data Protector. Reportez-vous à la section “Désinstallation du logiciel Data Protector” à la page 252.
- Comment ajouter ou supprimer des composants logiciels Data Protector. Reportez-vous à la section “Changement de composants logiciels Data Protector” à la page 268.

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 clients sont automatiquement ajoutés à la cellule. Dès que l'installation distante est terminée, le client devient membre de la cellule.

Quand faut-il importer ?

Certains clients, comme Novell NetWare, HP OpenVMS et Windows XP Edition familiale, doivent être importés dans la cellule après l'installation. **Importer** signifie ajouter manuellement un ordinateur à une cellule une fois le logiciel Data Protector installé. Une fois ajouté à une cellule Data Protector, le système devient un client Data Protector. Dès lors que le système est membre de la cellule, les informations relatives au nouveau client sont écrites dans la base IDB, située dans le Gestionnaire de cellule.

Un client ne peut être membre que d'une cellule. Si vous souhaitez déplacer un client vers une autre cellule, vous devez d'abord l'*exporter* à partir de sa cellule actuelle, puis l'*importer* dans la nouvelle cellule. Pour connaître la procédure à suivre pour exporter des clients, reportez-vous à la section "Exportation de clients d'une cellule" à la page 228.

IMPORTANT :

Après avoir installé les clients Data Protector et les avoir importés dans une cellule, il est vivement recommandé de les protéger afin d'empêcher l'accès d'autorités de cellule non autorisées. Reportez-vous à la section "Sécurisation de clients" à la page 235.

Comment importer ?

Vous importez un système client à l'aide de l'interface utilisateur graphique 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 client**.

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 34 à la page 223.

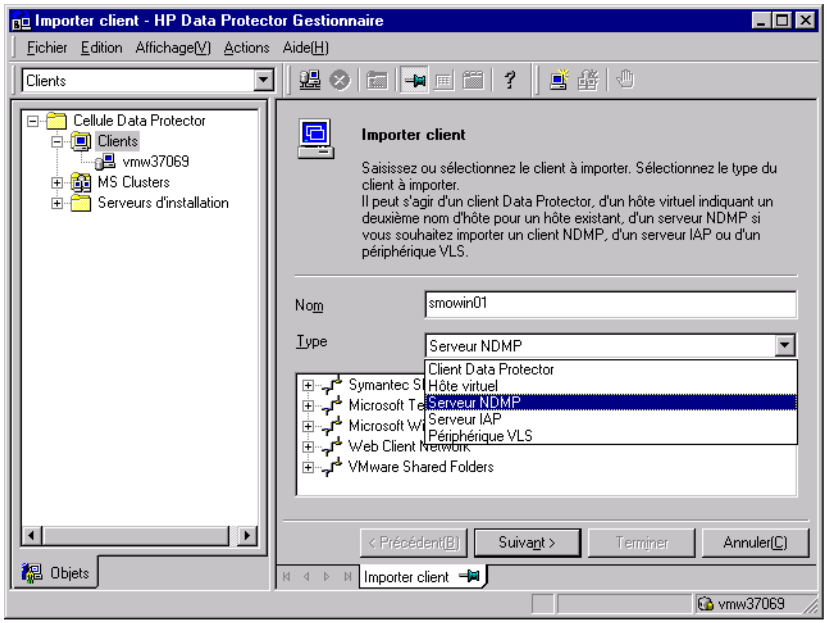


Figure 34 Importation d'un client vers la cellule

Si vous importez un client configuré avec plusieurs cartes réseau LAN, sélectionnez l'option **Hôte virtuel**. Avec cette option, vous devez importer tous les noms du même système.

Si vous importez un client NDMP, sélectionnez l'option **Serveur NDMP** puis cliquez sur **Suivant**. Spécifiez les informations relatives au serveur NDMP.

Si vous importez un client HP OpenVMS, saisissez son nom TCP/IP dans la zone de texte `Nom`.

Si vous importez un périphérique VLS, sélectionnez l'option **Périphérique VLS** puis cliquez sur **Suivant**. Spécifiez les informations relatives au périphérique VLS.

Si vous importez un hôte virtuel DAG Microsoft Exchange Server 2010 pour l'intégration de Data Protector avec Microsoft Exchange Server 2010, sélectionnez **Hôte virtuel**.

Si vous importez un client pour le composant Data Protector Intégration de l'environnement virtuel, sélectionnez **VMware ESX(i)** pour un système VMware

ESX(i) Server autonome, **VMware vCenter** pour un système VMware vCenter Server ou **Hyper-V** pour un système Microsoft Hyper-V. Cliquez sur **Suivant** et entrez les informations d'identification.

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, par exemple, il n'est pas installé sur un Gestionnaire de cellule.

  Dans ce cas, il ne sera pas possible d'installer à distance 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 utilisateur graphique 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 utilisateur graphique 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 la liste de contextes, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Serveurs d'installation**, puis cliquez sur **Importer Serveur d'installation** pour lancer l'assistant. Reportez-vous à la Figure 34 à la page 223.
3. Saisissez ou sélectionnez le nom du système que vous souhaitez importer. Cliquez sur **Terminer** pour importer le Serveur d'installation.

Importation d'un client compatible cluster dans une cellule

Après avoir installé le logiciel Data Protector en local sur un client compatible cluster, importez le serveur virtuel représentant le client compatible cluster dans la cellule Data Protector.

Configuration système requise

- Data Protector doit être installé sur tous les nœuds cluster.
- Tous les packages cluster doivent s'exécuter au sein du cluster.

Microsoft Cluster Server

Pour importer un client Microsoft Cluster Server dans la cellule Data Protector, procédez comme suit :

1. Dans Data Protector, affichez le contexte Clients.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **MS Clusters**, puis cliquez sur **Importer cluster**.

3. Saisissez le nom du serveur virtuel qui représente le client cluster à importer ou parcourez le réseau pour sélectionner le serveur virtuel. Reportez-vous à la Figure 35 à la page 226 .

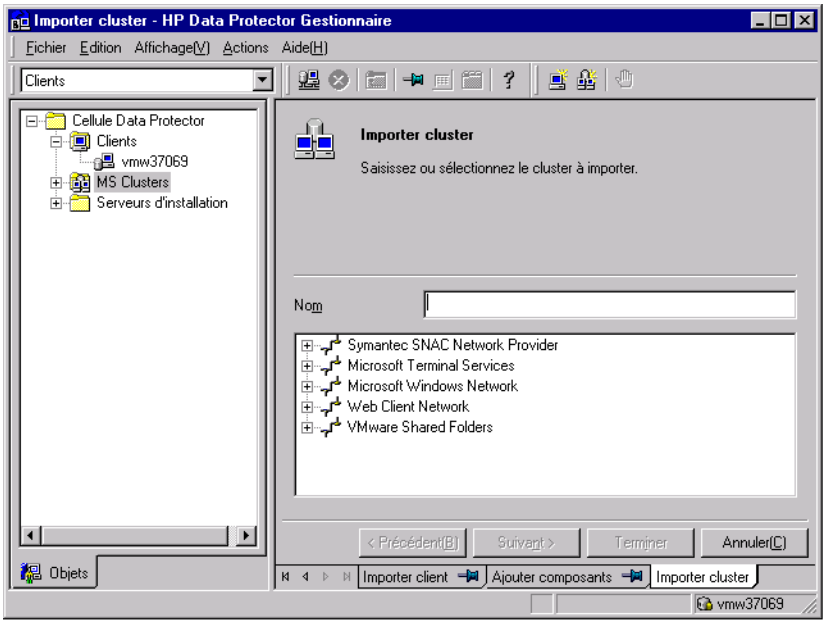


Figure 35 Importation d'un client Microsoft Cluster Server dans une cellule

4. Cliquez sur **Terminer** pour importer le client.

CONSEIL :

Pour importer un nœud de cluster ou un serveur virtuel particulier, cliquez avec le bouton droit de la souris sur son cluster dans la fenêtre de navigation, puis sélectionnez **Importer nœud cluster** ou **Importer serveur virtuel cluster**.

Autres clusters

Configuration requise pour les clusters Tru64

Avant d'importer les noms d'hôtes de clusters, assurez-vous que :

- Data Protector est installé sur le disque partagé dans le cluster
- Tous les nœuds cluster Tru64 s'exécutent au sein du cluster

- Data Protector Le processus `inetd` s'exécute sur chaque nœud

Procédure

Pour importer un client MC/ServiceGuard, Veritas, Tru64 Cluster, IBM HACMP Cluster ou Novell NetWare Cluster Services dans la cellule Data Protector, procédez comme suit :

1. Dans le Gestionnaire Data Protector, basculez vers le contexte Clients.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Clients**, puis cliquez sur **Importer client**.
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 de cluster. Reportez-vous à la Figure 36 à la page 228.
4. Cliquez sur **Terminer** pour importer le serveur virtuel.

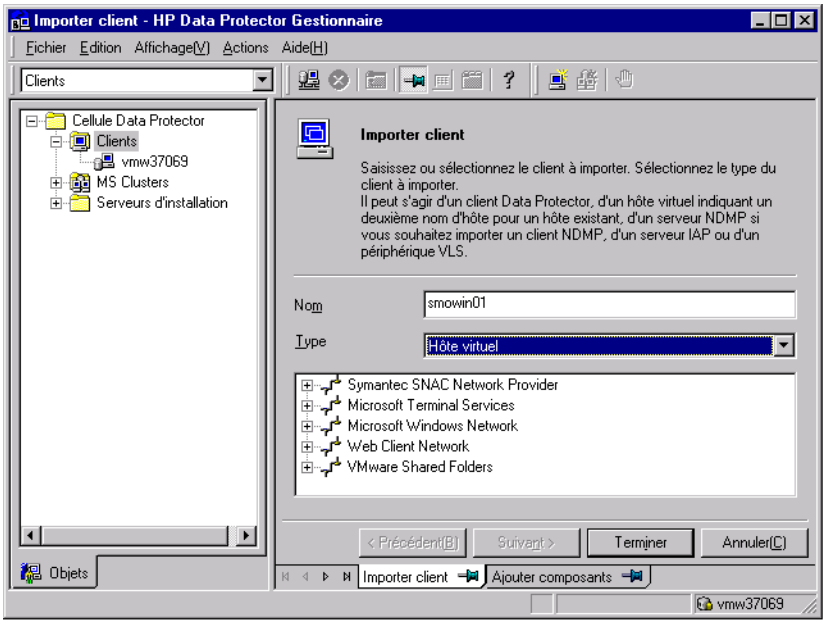


Figure 36 Importation d'un client MC/ServiceGuard, Veritas ou Novell NetWare Cluster Services dans une cellule

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 222

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 interne sur le Gestionnaire de cellule sans pour autant désinstaller le logiciel du client. Cette procédure peut être réalisée à l'aide de l'interface utilisateur graphique de 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 utilisateur graphique de Data Protector, procédez comme suit :

1. Dans le menu contextuel, cliquez sur **Clients**.

2. Dans la fenêtre de navigation, cliquez sur **Clients**, cliquez avec le bouton droit de la souris sur le système client à exporter, puis cliquez sur **Supprimer**. Reportez-vous à la Figure 37 à la page 230.

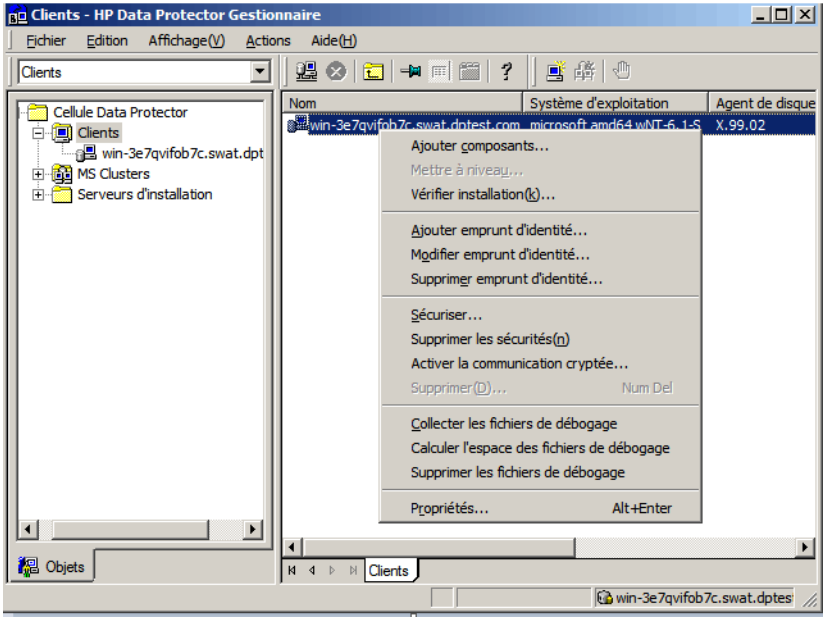


Figure 37 Exportation d'un système client

3. Un message vous demande si vous souhaitez également désinstaller le logiciel Data Protector. Cliquez sur **Non** pour exporter le client, puis sur **Terminer.**

Le client est supprimé de la liste dans la zone de résultats.

REMARQUE :

Vous ne pouvez pas exporter ou supprimer un client Data Protector si le Gestionnaire de cellule est installé sur le même système que le client à exporter. Toutefois, vous pouvez exporter les clients à partir des systèmes où seuls le client et le Serveur d'installation sont installés. Dans ce cas, le Serveur d'installation est supprimé de la cellule.

Clients Microsoft Cluster Server

Pour exporter un client Microsoft Cluster Server à partir de la cellule Data Protector, procédez comme suit :

1. Dans le menu contextuel, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, développez **MS Clusters**, cliquez avec le bouton droit de la souris sur le client cluster que vous souhaitez exporter, puis cliquez sur **Supprimer**.
3. Un message vous demande si vous souhaitez également désinstaller le logiciel Data Protector. Cliquez sur **Non** pour n'exporter que 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**.

A propos de 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, au 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
- Dans certains cas, une liste des clients qui accéderont au robot à distance.

IMPORTANT :

La liste doit contenir tous les noms d'hôte (ou adresses IP) possibles d'où les connexions peuvent provenir. Il est possible que plusieurs noms d'hôte soient nécessaires si l'un des clients mentionnés ci-dessus est multirésident (possède plusieurs cartes réseau et/ou plusieurs adresses IP) ou s'il s'agit d'un cluster.

Si la configuration DNS dans la cellule n'est pas uniforme, des considérations supplémentaires peuvent s'appliquer. Pour plus d'informations, reportez-vous à la section “Sécurisation de clients” à la page 235.

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 utilisateur graphique 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 Démarrer une spécification de sauvegarde” à la page 247.
- 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.
- Outre l'affectation de droits utilisateur d'après l'appartenance à un groupe d'utilisateurs, vous pouvez limiter les actions de certains groupes d'utilisateurs à des systèmes spécifiques de la cellule Data Protector. Pour mettre en œuvre cette stratégie, vous devez configurer le fichier user_restrictions. Pour plus d'informations, reportez-vous à l'aide en ligne.
- La configuration des utilisateurs dépend de la validation des utilisateurs (reportez-vous à la section “Vérification stricte du nom d'hôte” à la page 242). Une validation renforcée ne sert à rien si la configuration des utilisateurs n'est pas effectuée minutieusement ; inversement, la configuration utilisateur la plus étudiée peut être contournée si le niveau de validation n'est pas suffisant.
- Il est important que la liste des utilisateurs de Data Protector ne comporte pas de spécifications utilisateur "faibles".

REMARQUE :

La partie *hôte* d'une spécification utilisateur constitue la partie éprouvée (en particulier avec la validation renforcée), alors que les parties *utilisateur* et *groupe* ne peuvent pas être vérifiées de manière fiable. Tout utilisateur doté de droits utilisateur puissants doit être configuré en particulier pour le client qu'il utilisera pour l'administration de Data Protector. S'il utilise plusieurs clients, une entrée doit être ajoutée pour chaque client supplémentaire. Evitez de spécifier l'utilisateur ainsi : *utilisateur*, *groupe*, <*Tout*>. L'accès à l'un de ces systèmes doit être interdit aux utilisateurs non fiables.

Pour plus d'informations sur la configuration des utilisateurs, recherchez l'entrée suivante dans l'index de l'aide en ligne : "configuration, 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.

Bien qu'il ne soit pas toujours nécessaire de sécuriser chaque client de la cellule, il convient que les ordinateurs auxquels vont s'adresser les autres clients soient eux-mêmes sécurisés. Outre le Gestionnaire de cellule, les clients concernés sont le serveur d'installation et l'Agent de support.

La sécurité d'un Gestionnaire de cellule, puis celle de l'ensemble des clients de la cellule Data Protector, peut être renforcée grâce à l'activation des fonctions de communications de contrôle cryptées.

Pour plus d'informations, reportez-vous aux sections “Vérification stricte du nom d'hôte” à la page 242, “Sécurisation de clients” à la page 235 et “Echanges sécurisés” à la page 244.

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). L'autorisation ne

serait-ce que d'une connexion `anonyme` ou d'un accès `ftp` pourrait créer un risque au niveau de la sécurité globale.

- 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 la sauvegarde, la restauration, la copie de supports ou d'objets, la consolidation d'objets ou la vérification d'objet, les données sont généralement transférées via le réseau. Si la segmentation du réseau ne permet pas une séparation nette des parties fiables et non fiables du réseau, utilisez des périphériques connectés localement, des techniques de cryptage Data Protector ou une bibliothèque de codage personnalisée. Notez qu'après la modification de la bibliothèque de codage, vous devez réaliser une sauvegarde complète.
- Par ailleurs, l'activation des fonctions de communications de contrôle cryptées dans une cellule Data Protector permet d'empêcher tout accès non autorisé au système et renforce la sécurité.

Pour obtenir des informations sur les autres aspects liés à la sécurité, reportez-vous également à l'aide en ligne et au *Guide conceptuel HP Data Protector*.

Sécurisation de clients

Après avoir installé les clients Data Protector et les avoir importés dans une cellule, il est vivement recommandé de les protéger afin d'empêcher l'accès de clients non autorisés.

Data Protector vous permet de spécifier les autorités de cellule (Gestionnaire de cellule, MoM et Serveur d'installation) dont un client acceptera les requêtes sur le port Data Protector 5555. Ainsi, les autres ordinateurs ne seront pas en mesure d'accéder à ce client. Reportez-vous également à la section “Sécurité client” à la page 232.

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 utilisateur 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 ou les clients que vous voulez sécuriser, puis cliquez sur **Sécuriser**. Reportez-vous à la Figure 38 à la page 237.

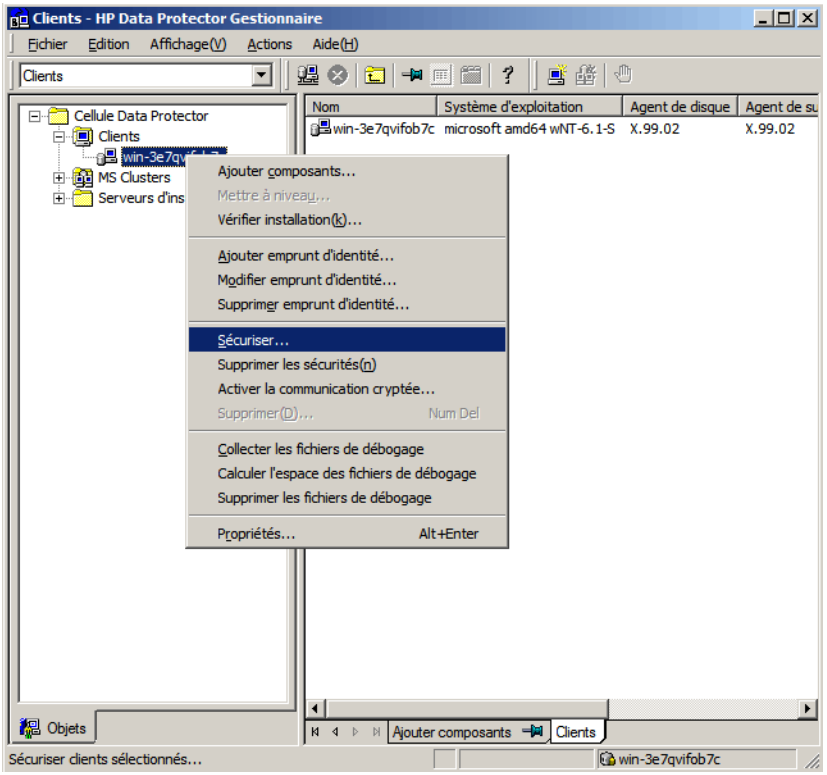


Figure 38 Sécurisation d'un client

3. Entrez les noms des systèmes qui auront accès aux clients sélectionnés ou recherchez ces systèmes en utilisant les onglets Réseau ou Recherche. Cliquez sur **Ajouter** pour ajouter chaque système à la liste. Reportez-vous à la Figure 39 à la page 238.

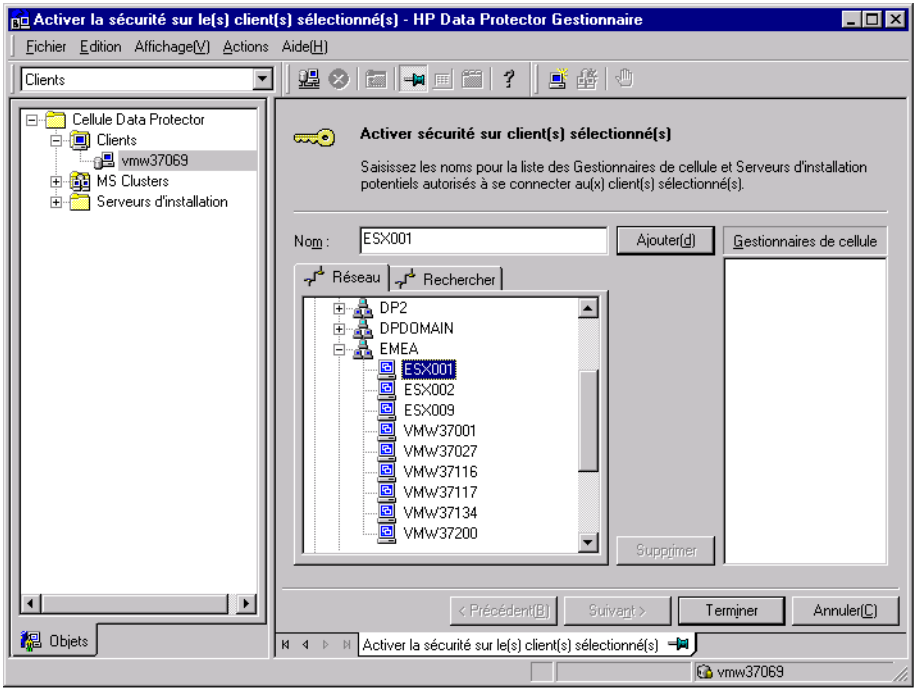


Figure 39 Activation de la sécurité sur les clients sélectionnés

Le Gestionnaire de cellule reçoit automatiquement une autorisation d'accès et il ajouté à la liste des clients fiables. Vous ne pouvez pas exclure le Gestionnaire de cellule de la liste.

4. Cliquez sur **Terminer** pour ajouter les systèmes sélectionnés au fichier `allow_hosts`.

Que se passe-t-il ?

Les clients vérifient la source de chaque requête provenant d'autres clients et n'autorisent que les requêtes reçues des clients sélectionnés dans la fenêtre Activer la sécurité sur le(s) client(s) sélectionné(s). Ces clients sont répertoriés dans le fichier `allow_hosts`. Si une demande est refusée, l'événement est consigné dans le fichier `inet.log` dans le répertoire suivant :

- Windows Vista, Windows 7, Windows Server 2008 : *données_programme_Data_Protector*\log
- Sur les autres systèmes Windows : *répertoire_Data_Protector*\log
- Sous HP-UX, Solaris et Linux : /var/opt/omni/log
- Autres systèmes UNIX et Mac OS X : /usr/omni/log

Pour sécuriser tous les clients de la cellule, procédez comme suit dans l'interface graphique de Data Protector :

1. Dans le menu contextuel, cliquez sur **Clients**.
2. Saisissez les noms des systèmes qui auront accès à tous les clients dans la cellule ou recherchez ces systèmes en utilisant les onglets Réseau (seulement si vous utilisez une interface graphique Windows) ou Recherche. Cliquez sur **Ajouter** pour ajouter chaque système à la liste. Reportez-vous à la Figure 40 à la page 239.

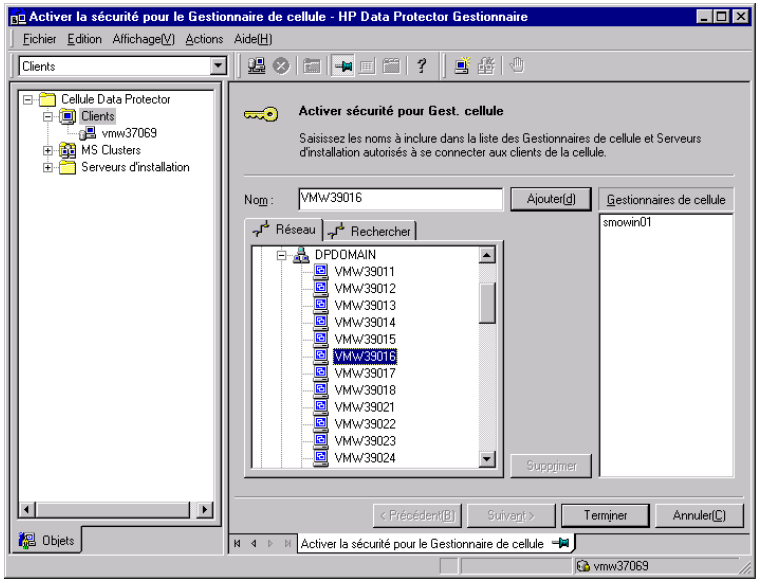


Figure 40 Activation de la sécurité pour tous les clients de la cellule

3. Cliquez sur **Terminer** pour ajouter les systèmes sélectionnés au fichier allow_hosts.

Que se passe-t-il ?

Les clients vérifient la source de chaque requête provenant d'autres clients et n'autorisent que les requêtes reçues des clients sélectionnés dans la fenêtre Activer la sécurité sur le Gestionnaire de cellule. Ces clients sont répertoriés dans le fichier `allow_hostsfichier allow_hostssécuritéfichier allow_hostsfichiersallow_hosts`. Si une demande est refusée, l'événement est consigné dans le fichier `inet.logfichier inet.logfichiers journauxinet.log` dans le répertoire suivant :

- Windows Vista, Windows 7, Windows Server 2008 : `données_programme_Data_Protector\log`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\log`
- Sous HP-UX, Solaris et Linux : `/var/opt/omni/log`
- Autres systèmes UNIX et Mac OS X : `/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 :

- Windows Vista, Windows 7 et Windows Server 2008 : `données_programme_Data_Protector\Config\client`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\Config\client`
- Sur les systèmes HP-UX, Solaris et Linux : `/etc/opt/omni/client`
- Autres systèmes UNIX et Mac OS X : `/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 dans un format codé sur deux octets (Unicode) ; sur les systèmes HP-UX, Solaris et Linux en revanche, ils sont dans un format codé sur un octet ou sur plusieurs octets (Shift-JIS, par exemple).

Journalisation excessive dans le fichier inet.log

Si les clients ne sont pas sécurisés et que le Gestionnaire de cellule est configuré dans l'environnement MC/ServiceGuard ou qu'il comporte plusieurs noms ou numéros IP, le fichier `inet.log` peut contenir plusieurs entrées dont le type est le suivant :

```
Une requête 0 a été émise par l'hôte nom.entreprise.com qui
n'est pas un Gestionnaire de cellule de ce client
```

Ces entrées résultent du fait que le client, qui n'est pas sécurisé, ne reconnaît que le nom d'hôte principal du Gestionnaire de cellule. Les demandes provenant de tous les autres clients sont autorisées et enregistrées dans le fichier `inet.log`.

Lorsqu'un client est sécurisé, les demandes provenant des clients répertoriés dans le fichier `allow_hosts` sont acceptées et ne sont donc pas enregistrées. Les demandes provenant d'autres clients sont refusées.

La sécurisation des clients peut être une solution permettant d'éviter les entrées inutiles dans les fichiers `inet.log`. Néanmoins, il est préférable de répertorier tous les noms de client possibles pour le Gestionnaire de cellule dans le fichier `allow_hosts` de chaque client. L'accès au client est ainsi garanti, même en cas de basculement.

Si cette solution est impossible dans votre environnement pour une raison quelconque, vous pouvez sécuriser les clients et spécifier * comme plage d'adresses IP pour les systèmes auxquels vous souhaitez autoriser l'accès. Cela signifie que vos clients accepteront les requêtes provenant de tous les systèmes (n'importe quelle adresse IP) et ne seront pratiquement pas sécurisés, mais que vous pourrez néanmoins résoudre le problème des connexions excessives.

Vérification stricte du nom d'hôte

Par défaut, le Gestionnaire de cellule utilise une méthode relativement simple pour valider les utilisateurs. Il utilise le nom d'hôte tel qu'il est connu du client lorsqu'une interface utilisateur ou un 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" (par exemple, ne faisant normalement pas l'objet d'attaques malveillantes).

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 des noms d'hôte

Le nom d'hôte utilisé par Data Protector pour la validation peut varier entre la validation de l'utilisateur par défaut et la vérification stricte du nom d'hôte dans les situations suivantes :

- La recherche DNS inverse renvoie un nom d'hôte différent. Ce renvoi peut être volontaire ou peut révéler une mauvaise configuration du client ou de la table de DNS inverse.
- Le client est multirésident (possède plusieurs cartes réseau et/ou plusieurs adresses IP). L'application de cette considération à un client multirésident particulier dépend du rôle joué par ce dernier sur le réseau et de la manière dont il est configuré dans le DNS.
- Le client est un cluster.

En raison de la nature des vérifications pouvant être effectuées avec ce paramétrage, une reconfiguration des utilisateurs de Data Protector peut s'avérer nécessaire. Les spécifications existantes des utilisateurs de Data Protector doivent être vérifiées afin de savoir si elles peuvent être attribuées à l'une des raisons mentionnées ci-dessus. Selon le cas, les spécifications existantes devront éventuellement être modifiées ou de nouvelles spécifications ajoutées pour toutes les adresses IP possibles d'où peuvent provenir des connexions.

Notez que les utilisateurs doivent également être reconfigurés lorsque vous revenez à la validation de l'utilisateur par défaut, si vous avez dû modifier les spécifications de l'utilisateur lorsque vous avez activé la vérification stricte du nom d'hôte. Il est par conséquent recommandé de choisir une validation d'utilisateur et de la conserver.

Pour que la recherche DNS inverse soit fiable, le serveur DNS doit être sécurisé. Vous devez empêcher l'accès physique et la connexion à l'ensemble du personnel non autorisé.

En configurant des utilisateurs avec des adresses IP au lieu de noms d'hôte, vous pouvez éviter certains problèmes de validation liés au DNS ; toutefois, une telle configuration est plus difficile à gérer.

Conditions requises

La validation renforcée ne donne pas automatiquement accès à certaines connexions internes. Par conséquent, lorsque cette validation est utilisée, un nouvel utilisateur doit être ajouté pour chacun des éléments suivants :

- Un Agent d'application (OB2BAR) sur des clients Windows. Pour les clients Windows, il faut ajouter l'utilisateur `SYSTEM`, `NT AUTHORITY`, *`client`* pour chaque client disposant d'un agent d'application installé. Remarquez que si `Inet` sur un client donné est configuré de manière à utiliser un compte spécifique, ce

compte doit déjà avoir été paramétré. Pour plus d'informations, recherchez l'entrée suivante dans l'index de l'aide en ligne : "Vérification stricte du nom d'hôte".

- Si vous utilisez la fonctionnalité de génération de rapports Web, l'utilisateur `java`, `applet`, *`nom_hôte`* doit être ajouté pour chaque nom d'hôte à partir duquel la fonctionnalité de génération de rapports Web sera utilisée. Notez que pour bénéficier pleinement de la fonctionnalité de génération de rapports Web, les utilisateurs doivent appartenir au même groupe `admin`. Par conséquent, ces clients doivent être sécurisés. De même, avant de mettre à disposition des utilisateurs des données ou la fonctionnalité de génération de rapports Web (par exemple, via un serveur Web), tenez compte des implications que la mise à la disposition générale de ce type de données engendre pour la sécurité.

Pour obtenir des informations détaillées sur la configuration utilisateur, recherchez l'entrée suivante dans l'index de l'aide en ligne : "configuration, utilisateurs".

Activation de la fonction

Pour activer la vérification stricte du nom d'hôte, définissez l'indicateur `StrictSecurityFlags 0x0001` dans le fichier d'options globales.

Pour plus d'informations sur le fichier d'options globales, reportez-vous au *Guide de dépannage HP Data Protector*.

Echanges sécurisés

Les communications de contrôle cryptées Data Protector permettent d'empêcher tout accès non autorisés aux clients dans la cellule Data Protector. L'interface utilisateur de Data Protector ou l'interface de ligne de commande permettent d'activer à distance les communications de contrôle cryptées pour tous les clients de la cellule Data Protector.

Pour activer les fonctions de communications de contrôle cryptées à partir de l'interface de ligne de commande, exécutez la commande suivante :

```
omnicc -encryption -enable
```

Pour plus d'informations, reportez-vous à la page `omnicc` du manuel ou au *Guide de référence de l'interface de ligne de commande HP Data Protector*.

IMPORTANT :

Vous pouvez activer les communications de contrôle cryptées à partir du Gestionnaire de cellule seulement ou de n'importe quel client de la cellule pour lequel les fonctions de communications de contrôle cryptées sont déjà activées.

Activation des communications de contrôle cryptées

Pour activer les fonctions de communications de contrôle cryptées via l'interface utilisateur de Data Protector, procédez comme suit :

REMARQUE :

Vous devez tout d'abord activer les communications de contrôle cryptées sur un Gestionnaire de cellule, puis sur les clients de la cellule.

1. Dans le menu contextuel, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, développez **Cellule Data Protector**, puis **Clients**. Tous les clients sont affichés.
3. Cliquez sur le client à modifier.
4. Dans la page de propriétés Connexion, sélectionnez l'option **Communication contrôlée par cryptage**.
5. Dans la liste déroulante **Chaîne de certificats**, sélectionnez le certificat.
6. Dans la liste déroulante **Clé privée** , sélectionnez la clé privée.
7. Dans la liste déroulante **Certificat approuvé**, sélectionnez le certificat.
8. Cliquez sur **Appliquer** pour enregistrer les modifications.

Pour activer les fonctions de communications de contrôle cryptées sur plusieurs clients via l'interface utilisateur de Data Protector, procédez comme suit :

1. Dans le menu contextuel, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, développez **Cellule Data Protector**, puis **Clients**. Tous les clients sont affichés.
3. Cliquez avec le bouton droit sur le client à partir duquel vous voulez activer les communications de contrôle cryptées, puis cliquez sur **Activer la communication cryptée**.

4. Sélectionnez un ou plusieurs clients pour lesquels activer les communications de contrôle cryptées. Cliquez sur **Suivant**.
5. Dans la liste déroulante **Chaîne de certificats**, sélectionnez le certificat.
6. Dans la liste déroulante **Clé privée** , sélectionnez la clé privée.
7. Dans la liste déroulante **Certificat approuvé**, sélectionnez le certificat.
8. Cliquez sur **Terminer** pour enregistrer les modifications.

Que se passe-t-il ?

Le cryptage est activé client par client, ce qui signifie qu'il est soit activé soit désactivé pour toutes les communications de contrôle avec le client sélectionné.

Ajout d'un client à la liste Exceptions de sécurité

Certains clients qui ne sont pas supposés communiquer de façon confidentielle peuvent être placés dans une liste d'exceptions du Gestionnaire de cellule, ce qui leur permet de communiquer en mode non crypté.

Pour ajouter un client à la liste Exceptions de sécurité via l'interface utilisateur de Data Protector, procédez comme suit :

1. Dans le menu contextuel, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, développez **Cellule Data Protector**, puis **Clients**. Tous les clients sont affichés.
3. Cliquez sur le Gestionnaire de cellule à modifier.
4. Saisissez les noms des systèmes qui seront ajoutés à la liste Exceptions de sécurité dans la cellule ou recherchez-les à l'aide des onglets **Réseau** (seulement si vous utilisez une interface utilisateur Windows) ou **Recherche**.
5. Cliquez sur **Ajouter** pour ajouter les systèmes à la liste, puis sur **Appliquer** pour enregistrer les modifications.

Fichier de `configuration du serveur`

Les clients acceptés en mode texte brut sont enregistrés dans le fichier de `configuration du serveur`, disponible dans le répertoire suivant du Gestionnaire de cellule :

- Windows Vista, Windows Server 2008 : `données_programme_Data_Protector\Config\server\config`

- Autres systèmes Windows : `répertoire_Data_Protector\Config\server\config`
- Systèmes HP-UX, Solaris et Linux : `/etc/opt/omni/server/config`

Pour retirer un système de la liste Exceptions de sécurité, suivez les étapes 1 à 4 et cliquez sur **Supprimer**, puis sur **Appliquer** pour enregistrer les modifications.

Limite

- La communication entre un client utilisant les fonctions de communications de contrôle standard et un client utilisant les fonctions de communications de contrôle cryptées n'est pas prise en charge. Autrement dit, les opérations de Data Protector ne seront pas exécutées (par exemple, l'installation à distance à partir d'un Serveur d'installation, qui utilise les communications de contrôle standard, sur le client qui utilise les communications de contrôle cryptées ne peut pas aboutir).

  En revanche, le Gestionnaire de cellule peut communiquer avec les deux types de clients dans la cellule Data Protector.

Droit utilisateur Démarrer une 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 utilisateur graphique. 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 utilisateur graphique et il est en mesure de démarrer une spécification de sauvegarde ou une sauvegarde interactive.

Il n'est pas toujours souhaitable de permettre aux utilisateurs d'effectuer des sauvegardes interactives. Pour autoriser des sauvegardes interactives uniquement aux utilisateurs ayant le droit d'enregistrer une spécification de sauvegarde, paramétrez l'indicateur StrictSecurityFlags 0x0200 dans le fichier d'options globales.

Pour plus d'informations sur le fichier d'options globales, reportez-vous au *Guide de dépannage HP Data Protector*.

Masquer le contenu des spécifications de sauvegarde

Dans un environnement hautement sécurisé, le contenu des spécifications de sauvegarde enregistrées peut être considéré comme sensible, voire confidentiel. Il est possible de configurer Data Protector pour qu'il dissimule le contenu des spécifications de sauvegarde à tous les utilisateurs, à l'exception de ceux qui disposent des droits d'utilisateur *Enregistrer spécification de sauvegarde*. Pour ce faire, réglez l'indicateur StrictSecurityFlags sur 0x0400 dans le fichier d'options globales.

Pour plus d'informations sur le fichier d'options globales, reportez-vous au *Guide de dépannage HP Data Protector*.

Groupements d'hôtes approuvés

La fonctionnalité de groupement d'hôtes approuvés réduit la nécessité d'accorder des droits d'utilisateur Restaurer vers autres clients lorsqu'ils doivent seulement restaurer les données d'un client à un autre parmi un nombre limité de clients. Vous pouvez définir des groupes d'hôtes qui échangeront des données en toute confiance.

Les groupements d'hôtes approuvés sont habituellement utilisés dans les situations suivantes :

- Pour les clients d'un même cluster (noeuds et serveur virtuel).
- Si le nom d'hôte d'un client est modifié et que les données des anciens objets sauvegarde doivent être restaurées.
- En cas d'incohérence entre le nom d'hôte du client et les objets sauvegarde en raison de problèmes liés au DNS.
- Si un utilisateur détient plusieurs clients et doit restaurer les données d'un client vers un autre.
- Lors de la migration de données d'un hôte vers un autre.

Configuration

Pour configurer les groupements d'hôtes approuvés, sur le Gestionnaire de cellule, créez le fichier données_programme_Data_Protector\Config\Server\cell\host_trusts (Windows Server 2008), `répertoire_Data_Protector\Config\Server\cell\host_trusts` (autres systèmes Windows) ou `/etc/opt/omni/server/cell/host_trusts` (systèmes UNIX).

Les groupes d'hôtes qui se font confiance mutuellement sont définis en tant que listes de noms d'hôtes placées entre crochets. Par exemple :

Exemple

```
GROUP="cluster.domain.com"
{
cluster.domain.com
node1.domain.com
node2.domain.com
}
GROUP="Bajo"
{
computer.domain.com
anothercomputer.domain.com
}
```

Surveillance des événements de sécurité

Si vous rencontrez un problème lors de l'utilisation de Data Protector, vous pouvez consulter les informations des fichiers journaux pour en trouver la cause. Par exemple, les événements consignés pourront vous aider à déterminer les utilisateurs ou clients incorrectement configurés.

Evénements de sécurité client

Les événements de sécurité client sont consignés dans le fichier `inet.log` sur chaque client de la cellule :

- Windows Vista, Windows 7 et Windows Server 2008 : `données_programme_Data_Protector\log`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\log`
- Sous HP-UX, Solaris et Linux : `/var/opt/omni/log`
- Autres systèmes UNIX et Mac OS X : `/usr/omni/log`

Evénements de sécurité Gestionnaire de cellule

Les événements de sécurité du Gestionnaire de cellule sont consignés dans le fichier `security.log` sur le Gestionnaire de cellule :

- Sous Windows Server 2008 : *`données_programme_Data_Protector`*`\log\server`
- Sur les autres systèmes Windows : *`répertoire_Data_Protector`*`\log\server`

- Sur les systèmes UNIX : `/var/opt/omni/server/log`

Contrôle des correctifs Data Protector installés

Vous pouvez vérifier quels correctifs Data Protector sont installés sur chaque système de la cellule.

Condition préalable

Pour utiliser cette fonctionnalité, le composant Interface utilisateur ou le client de l'interface Java doit être installé.

REMARQUE :

Si vous avez installé un correctif spécifique pour un site par le passé, celui-ci sera toujours répertorié dans le rapport des correctifs, même s'il a été par la suite inclus dans d'autres correctifs.

Pour vérifier quels sont les correctifs Data Protector installés sur un système donné dans une cellule, utilisez l'interface utilisateur graphique ou l'interface de ligne de commande de Data Protector.

Limites

Les limites relatives au contrôle des correctifs sont les suivantes :

- Le contrôle des correctifs vérifie quels correctifs sont installés uniquement sur les membres de la même cellule.

Contrôle des correctifs Data Protector à l'aide de l'interface utilisateur graphique

Pour vérifier quels sont les correctifs installés sur un client en particulier à l'aide de l'interface utilisateur graphique 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**.

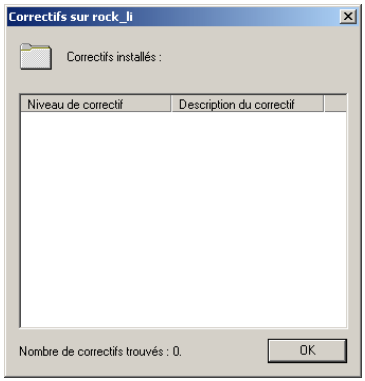


Figure 41 Vérification des correctifs installés

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 utilisateur graphique de Data Protector, exécutez la commande `omnicheck -patches -host` *`nom_hôte`* à partir du répertoire suivant :

- Sous Windows : *`répertoire_Data_Protector`*`\bin`
- Sous UNIX :`/opt/omni/bin`

où *`nom_hôte`* est le nom du système à vérifier.

Pour en savoir plus sur la commande `omnicheck`, reportez-vous à la page `omnicheck` du manuel.

Désinstallation du logiciel Data Protector

Si la configuration de votre système change, vous souhaiterez peut-être désinstaller Data Protector du système ou retirer certains de ses composants logiciels.

La désinstallation consiste à supprimer tous les composants Data Protector du système, dont *toutes* les références à ce système provenant de la base de données IDB sur l'ordinateur du Gestionnaire de cellule. Cependant, les données de configuration de Data Protector restent sur le système par défaut pour que vous puissiez les utiliser pour la prochaine mise à niveau de Data Protector. Si vous souhaitez supprimer les données de configuration après la désinstallation du logiciel Data Protector, supprimez les répertoires dans lesquels Data Protector a été installé.

Si le répertoire dans lequel Data Protector est installé comporte d'autres données, vérifiez que vous les avez copiées dans un autre emplacement avant de procéder à la désinstallation de Data Protector. Dans le cas contraire, elles seront supprimées au moment de la désinstallation.

La désinstallation du logiciel Data Protector d'une cellule se déroule comme suit :

1. Désinstallation du logiciel client Data Protector à l'aide de l'interface utilisateur graphique. Reportez-vous à la section "Désinstallation d'un client Data Protector" à la page 253.
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 254.

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 268.

Sous UNIX, vous pouvez également supprimer manuellement le logiciel Data Protector. Reportez-vous à la section "Suppression manuelle du logiciel Data Protector sous UNIX" à la page 267.

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 à désinstaller. Une fois le système exporté, Data Protector ne peut plus utiliser ses périphériques de sauvegarde dans la cellule d'origine.

Désinstallation d'un client Data Protector

REMARQUE :

La procédure de désinstallation à distance nécessite que le Serveur d'installation soit installé pour les plates-formes à partir desquelles vous désinstallez le logiciel de Data Protector.

Pour désinstaller un client à distance, procédez comme suit dans l'interface graphique de Data Protector :

1. Dans le menu contextuel, sélectionnez **Clients**.
2. Dans la fenêtre de navigation, développez **Clients**, cliquez avec le bouton droit de la souris sur le client à désinstaller, puis cliquez sur **Supprimer**. Un message vous demande si vous souhaitez également désinstaller le logiciel Data Protector.
3. Cliquez sur **Oui** pour désinstaller tous les composants logiciels du client, puis sur **Terminer**.

Le client sera supprimé de la liste figurant dans la zone de résultats et le logiciel Data Protector sera supprimé de son disque dur.

Notez que les données de configuration de Data Protector restent sur le système client. Si vous souhaitez supprimer les données de configuration, supprimez les répertoires dans lesquels Data Protector a été installé.

La désinstallation de Data Protector supprime également le client de l'interface Java. A moins que vous ne décochiez l'option **Supprimer définitivement les données de configuration** lorsque vous désinstallez Data Protector, les données de configuration de l'interface Java restent sur le système.

Clients cluster

Si votre environnement Data Protector comprend des clients compatibles cluster dans et que vous souhaitez les désinstaller, vous devez le faire localement. La procédure est la même que pour la désinstallation du Gestionnaire de cellule ou du Serveur

d'installation. Reportez-vous à la section "Désinstallation du Gestionnaire de cellule et du Serveur d'installation" à la page 254.

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 HP OpenVMS

Un client OpenVMS Data Protector ne peut être supprimé à distance avec un Serveur d'installation. Il doit être désinstallé localement.

Pour désinstaller un client Data Protector d'un système OpenVMS, procédez comme suit :

1. Commencez par exporter le client concerné à partir de la cellule Data Protector dans l'interface graphique de ce dernier, comme l'indique la section "Exportation de clients d'une cellule" à la page 228.

   A la question demandant si vous souhaitez désinstaller également le logiciel Data Protector, répondez **Non**.

2. Pour supprimer le logiciel client Data Protector, connectez-vous au compte `SYSTEM` du client OpenVMS et exécutez la commande suivante : `$ PRODUCT REMOVE DP`. Répondez à l'invite en indiquant `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 de désinstallation du Gestionnaire de cellule et du Serveur d'installation Data Protector des systèmes Windows, HP-UX, Solaris et Linux.

Désinstallation sur les systèmes Windows

Désinstallation d'un cluster de serveur Microsoft

Si vous avez installé l'utilitaire HP AutoPass en même temps que Data Protector sur un noeud de serveur de cluster Microsoft, vous devez désinstaller Data Protector de ce même noeud ; dans le cas contraire, AutoPass *ne* sera *pas* désinstallé.

Pour désinstaller le logiciel Data Protector d'un système Windows, procédez comme suit :

1. Assurez-vous que toutes les sessions de Data Protector sont terminées et que vous avez quitté l'interface utilisateur graphique.
2. Dans le Panneau de configuration de Windows, cliquez sur **Ajout/Suppression de programmes**.

3. Selon que vous ayez installé HP AutoPass ou non et selon que vous souhaitiez supprimer les données de configuration de Data Protector ou non, différentes actions sont possibles.

IMPORTANT :

Si vous laissez les données de configuration de Data Protector sur le système après la désinstallation et que vous réinstallez plus tard une version antérieure du Gestionnaire de cellule Data Protector à celle qui était installée, notez que les données de configuration ne seront pas compatibles.

Pour installer correctement une version antérieure, lors de l'installation, choisissez l'option qui supprime les données de configuration.

Pour ce faire, procédez comme suit :

- Si l'utilitaire AutoPass a été installé avec Data Protector :

  Sélectionnez **HP Data Protector 6.20** et cliquez sur **Changer** puis sur **Suivant**. Dans la boîte de dialogue Maintenance du programme, sélectionnez **Supprimer**. Pour supprimer définitivement les données de configuration de Data Protector, sélectionnez **Supprimer définitivement les données de configuration**. Dans le cas contraire, cliquez sur **Suivant**.

  Si AutoPass a été installé en même temps que Data Protector et que Data Protector est la seule application qui l'utilise, AutoPass est supprimé. Dans le cas contraire, seul l'enregistrement d'AutoPass auprès de Data Protector est annulé, mais l'utilitaire reste installé. Pour supprimer manuellement AutoPass, exécutez :

  ```
  msiexec.exe /X ID_interface graphique_package /qr
  INSTALLSTANDALONE=1
  ```

  Vous trouverez l'ID d'interface sous l'entrée du registre `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\HpOvLic`.

- Si AutoPass n'a pas été installé :
  - Pour désinstaller Data Protector et conserver les données de configuration Data Protector sur le système, sélectionnez **HP Data Protector 6.20** et cliquez sur **Supprimer**.
  - Pour désinstaller Data Protector et supprimer ses données de configuration, sélectionnez **HP Data Protector 6.20**, cliquez sur **Changer** puis sur **Suivant**. Dans la boîte de dialogue Maintenance du programme, sélectionnez **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 sur les systèmes HP-UX

IMPORTANT :

Si vous laissez les données de configuration de Data Protector sur le système après la désinstallation et que vous réinstallez plus tard une version antérieure du Gestionnaire de cellule Data Protector à celle qui était installée, notez que les données de configuration ne seront pas compatibles.

Pour installer correctement une version antérieure, après la désinstallation, supprimez les répertoires Data Protector de votre système.

Avant de commencer à désinstaller le logiciel Data Protector, arrêtez tous les processus Data Protector en cours d'exécution sur le système du Gestionnaire de cellule et/ou du Serveur d'installation :

1. Connectez-vous en tant que root et exécutez la commande `omnisv -stop` à partir du répertoire `/opt/omni/sbin`.
2. Entrez la commande `ps -ef | grep omni` pour vérifier si tous les processus ont bien été arrêtés. Aucun processus Data Protector ne doit être affiché après 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`*`ID_processus`* avant de procéder à la désinstallation.
3. Exécutez `/usr/sbin/swremove DATA-PROTECTOR` pour désinstaller le logiciel Data Protector.
4. L'utilitaire HP AutoPass n'est pas supprimé lors de la désinstallation de Data Protector. Vous pouvez le supprimer manuellement en exécutant la commande `/usr/sbin/swremove HPOVLIC` en tant qu'utilisateur root.

Pour supprimer les répertoires restants de Data Protector de votre système, reportez-vous à la section "Suppression manuelle du logiciel Data Protector sous UNIX" à la page 267.

Désinstallation du Gestionnaire de cellule et/ou du Serveur d'installation configuré(s) sur MC/ServiceGuard

Si votre Gestionnaire de cellule et/ou votre Serveur d'installation sont configurés sur un cluster MC/ServiceGuard, procédez comme suit pour désinstaller le logiciel.

Nœud principal

Connectez-vous au nœud principal et procédez comme suit :

1. Arrêtez le package Data Protector :

   ```
   cmhaltpkg nom_pkg
   ```

   où `nom_pkg` correspond au nom du package de clusters.

   Par exemple :

   ```
   cmhaltpkg ob2cl
   ```

2. Désactivez le mode cluster pour le groupe de volumes :

   ```
   vgchange -c n nom_gv
   ```

   (où `nom_gv` correspond au nom du chemin du groupe de volumes placé dans le sous-répertoire du répertoire `/dev`).

   Par exemple :

   ```
   vgchange -c n /dev/vg_ob2cm
   ```

3. Activez le groupe de volumes :

   ```
   vgchange -a y -q y nom_gv
   ```

   Par exemple :

   ```
   vgchange -a y -q y /dev/vg_ob2cm
   ```

4. Montez le volume logique sur le disque partagé :

   ```
   mount chemin_vl disque_partagé
   ```

   (où `chemin_vl` correspond au nom de chemin du volume logique et où `disque_partagé` correspond au point de montage ou répertoire partagé).

   Par exemple :

   ```
   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
   ```

5. Supprimez Data Protector à l'aide de l'outil swremove.

6. Supprimez les liens programmables :

   ```
   rm /etc/opt/omni
   rm /var/opt/omni
   ```

7. Supprimez les répertoires de sauvegarde :

   ```
   rm -rf /etc/opt/omni.save
   rm -rf /var/opt/omni.save
   ```

8. Supprimez le répertoire Data Protector et son contenu :

   ```
   rm -rf /opt/omni
   ```

9. Vous pouvez supprimer l'utilitaire HP AutoPass en exécutant la commande `/usr/sbin/swremove HPOVLIC` en tant qu'utilisateur root.
10. Démontez le disque partagé :

    ```
    umount disque_partagé
    ```

    Par exemple :

    ```
    umount /omni_shared
    ```

11. Désactivez le groupe de volumes :

    ```
    vgchange -a n nom_gv
    ```

    Par exemple :

    ```
    vgchange -a n /dev/vg_ob2cm
    ```

Nœud secondaire

Connectez-vous au nœud secondaire et procédez comme suit :

1. Activez le groupe de volumes :

   ```
   vgchange -a y nom_gv
   ```

2. Montez le disque partagé :

   ```
   mount chemin_vl disque_partagé
   ```

3. Supprimez Data Protector à l'aide de l'outil `swremove`.
4. Supprimez les liens programmables :

   ```
   rm /etc/opt/omni
   rm /var/opt/omni
   ```

5. Supprimez les répertoires de sauvegarde :

   ```
   rm -rf /etc/opt/omni.save
   rm -rf /var/opt/omni.save
   ```

6. Supprimez le répertoire Data Protector et son contenu :

   ```
   rm -rf /opt/omni
   ```

7. Supprimez les répertoires du système de fichiers partagé :

   ```
   rm -rf disque_partagé/etc_opt_omni
   rm -rf disque_partagé/var_opt_omni
   ```

   Par exemple :

   ```
   rm -rf /omni_shared/etc_opt_omni
   rm -rf /omni_shared/etc_opt_omni
   ```

8. Vous pouvez supprimer l'utilitaire HP AutoPass en exécutant la commande `/usr/sbin/swremove HPOVLIC` en tant qu'utilisateur root.

9. Démontez le disque partagé :

   `umount` *`disque_partagé`*

10. Désactivez le groupe de volumes :

    `vgchange -a n` *`nom_gv`*

Data Protector est complètement supprimé du système.

Désinstallation dans les systèmes Solaris

Gestionnaire de cellule

Le Gestionnaire de cellule pour Solaris est toujours installé en local, à l'aide de la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé en local à l'aide de l'utilitaire `pkgrm`.

IMPORTANT :

Si vous laissez les données de configuration de Data Protector sur le système après la désinstallation et que vous réinstallez plus tard une version antérieure du Gestionnaire de cellule Data Protector à celle qui était installée, notez que les données de configuration ne seront pas compatibles.

Pour installer correctement une version antérieure, après la désinstallation, supprimez les répertoires Data Protector de votre système.

Pour désinstaller le Gestionnaire de cellule Data Protector, procédez comme suit :

1. Assurez-vous que vous avez terminé toutes les sessions de Data Protector et quitté l'interface utilisateur graphique.
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 utilisateur graphique et l'interface de ligne de commande

   Si des clients Data Protector ou Serveur d'installation sont aussi installés sur le système, les autres packages seront également répertoriés.

REMARQUE :

Si vous souhaitez laisser tout autre composant Data Protector installé, vous devez conserver le package OB2-CORE car il est indispensable au fonctionnement des autres packages.

3. Supprimez, dans l'ordre inverse de celui où ils ont été installés, les packages indiqués dans l'Étape 2 à la page 261 à l'aide de la commande `pkgrm nom du package` et suivez les instructions qui apparaissent sur la ligne de commande.

4. L'utilitaire HP AutoPass n'est pas supprimé lors de la désinstallation de Data Protector. Vous pouvez le supprimer manuellement en exécutant les commandes suivantes en tant qu'utilisateur root :

   ```
   swremove HPOvLic
   ```

Serveur d'installation

Le Serveur d'installation pour UNIX sur Solaris est toujours installé en local à l'aide de la commande `omnisetup.sh`.. Par conséquent, il doit être désinstallé en local à l'aide de l'utilitaire `pkgrm`.

Pour désinstaller le Serveur d'installation Data Protector, procédez comme suit :

1. Veillez à terminer toutes les sessions de Data Protector et à quitter l'interface 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-CFP	Paquets de Serveur d'installation communs à tous les systèmes UNIX.
OB2-CCP	Paquets d'installation à distance de la console de cellule pour tous les systèmes UNIX.
OB2-DAP	Paquets d'installation à distance de l'Agent de disque pour tous les systèmes UNIX.
OB2-MAP	Paquets d'installation à distance de l'Agent de support pour tous les systèmes UNIX.

   Si d'autres composants Data Protector sont installés sur le système, ils seront également répertoriés.

   Pour obtenir la liste complète des composants et de leurs dépendances, reportez-vous au Tableau 9 à la page 271.

REMARQUE :

Si vous souhaitez laisser tout autre composant Data Protector installé, vous devez conserver le package OB2-CORE car il est indispensable au fonctionnement des autres packages.

3. Supprimez dans l'ordre inverse de celui où ils ont été installés les packages mentionnés dans l'étape précédente par la commande `pkgrm` *`nom du package`* et suivez les instructions qui apparaissent sur la ligne de commande.

Désinstallation dans les systèmes Linux

Gestionnaire de cellule

Le Gestionnaire de cellule pour Linux est toujours installé en local, à l'aide de la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé en local à l'aide de l'utilitaire `rpm`.

IMPORTANT :

Si vous laissez les données de configuration de Data Protector sur le système après la désinstallation et que vous réinstallez plus tard une version antérieure du Gestionnaire de cellule Data Protector à celle qui était installée, notez que les données de configuration ne seront pas compatibles.

Pour installer correctement une version antérieure, après la désinstallation, supprimez les répertoires Data Protector de votre système.

Pour désinstaller le Gestionnaire de cellule Data Protector, procédez comme suit :

1. Assurez-vous que vous avez terminé toutes les sessions de Data Protector et quitté l'interface utilisateur graphique.

2. Entrez la commande `rpm -qa | grep OB2` pour répertorier tous les packages Data Protector installés sur le Gestionnaire de cellule.

   Les packages associés au Gestionnaire de cellule se répartissent comme suit :

OB2-CORE	Logiciel central Data Protector
OB2-CORE-IS	Logiciel du Serveur d'installation
OB2-CS	Logiciel du Gestionnaire de cellule
OB2-CC	Logiciel de la console de cellule, contenant l'interface de ligne de commande.

   Si des clients Data Protector ou Serveur d'installation sont aussi installés sur le système, les autres packages seront également répertoriés.

   REMARQUE :

   Si vous souhaitez laisser tout autre composant Data Protector installé, vous devez conserver le package OB2-CORE car il est indispensable au fonctionnement des autres packages.

3. Supprimez dans l'ordre inverse de celui où il ont été installés les packages mentionnés dans l'étape précédente par la commande `rpm -e`*`nom du package`* et suivez les instructions qui apparaissent sur la ligne de commande.

Serveur d'installation

Le Serveur d'installation pour UNIX sous Linux est toujours installé en local à l'aide de la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé en local à l'aide de l'utilitaire `rpm`.

Pour désinstaller le Serveur d'installation Data Protector, procédez comme suit :

1. Assurez-vous que toutes les sessions de Data Protector sont terminées et que vous avez quitté l'interface utilisateur graphique.

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-CFP	Paquets de Serveur d'installation communs à tous les systèmes UNIX.
OB2-CCP	Paquets d'installation à distance de la console de cellule pour tous les systèmes UNIX.
OB2-DAP	Paquets d'installation à distance de l'Agent de disque pour tous les systèmes UNIX.
OB2-MAP	Paquets d'installation à distance de l'Agent de support pour tous les systèmes UNIX.

   Si d'autres composants Data Protector sont installés sur le système, ils seront également répertoriés.

   Pour obtenir la liste complète des composants et de leurs dépendances, reportez-vous au Tableau 10 à la page 271.

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 228.

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 et Mac OS X :

Supprimez les fichiers du répertoire suivant, puis supprimez le répertoire à l'aide de la commande `rm` :

```
rm -fr /usr/omni
```

Changement de composants logiciels Data Protector

Cette section décrit la procédure de suppression et d'ajout de composants logiciels Data Protector sur les systèmes Windows, HP-UX, Solaris et Linux. Pour obtenir la liste des composants Data Protector pris en charge selon les systèmes d'exploitation, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

Les composants logiciels Data Protector peuvent être ajoutés sur le Gestionnaire de cellule ou sur un client à l'aide de l'interface utilisateur graphique 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 83.

Les composants Data Protector peuvent être supprimés en local sur le Gestionnaire de cellule ou sur un client.

Sur les systèmes Windows

Pour ajouter ou supprimer des composants logiciels Data Protector sous Windows, procédez comme suit :

1. Dans le Panneau de configuration de Windows, cliquez sur **Ajout/Suppression de programmes**.
2. Sélectionnez **HP Data Protector 6.20** et cliquez sur **Modifier**.
3. Cliquez sur **Suivant**.
4. Dans la fenêtre Maintenance du programme, cliquez sur **Modifier**, puis sur **Suivant**.
5. Dans la fenêtre Installation personnalisée, sélectionnez les composants à ajouter et/ou désélectionnez les composants à supprimer. Cliquez sur **Suivant**.
6. Cliquez sur **Installer** pour lancer l'installation ou la suppression des composants logiciels.
7. Lorsque l'installation est terminée, cliquez sur **Terminer**.

Clients compatibles cluster

Si vous modifiez les composants logiciels de Data Protector sur les clients compatibles cluster, vous devez le faire localement, à partir du DVD-ROM, sur chaque nœud de cluster. Ensuite, vous devez importer manuellement le nom d'hôte du serveur virtuel dans la cellule Data Protector à l'aide de l'interface utilisateur.

Sur les systèmes HP-UX

Vous pouvez ajouter de nouveaux composants à l'aide de la fonctionnalité Serveur d'installation. Sur les systèmes HP-UX, certains composants Data Protector dépendent les uns des autres et ne pourront fonctionner correctement si vous supprimez l'un d'entre eux. Le tableau ci-dessous présente les composants et leurs interdépendances :

Tableau 8 Dépendances de composants logiciels Data Protector sous HP-UX

Composants	**dépendent de...**
Gestionnaire de cellule	
OMNI-CC	OMNI-CORE
OMNI-CS	OMNI-CORE, OMNI-CC
OMNI-DA, OMNI-MA, OMNI-JAVAGUI, OMNI-DOCS	OMNI-CORE
Serveur d'installation	
OMNI-CORE-IS	OMNI-CORE
OMNI-CF-P	OMNI-CORE-IS
OMNI-CC-P, OMNI-JGUI-P, OMNI-DA-P, OMNI-MA-P, OMNI-NDMP-P, OMNI-AUTODR-P, OMNI-DOCS-P, OMNI-CHS-LS-P, OMNI-FRA-LS-P, OMNI-JPN-LS-P, OMNI-PEGASUS-P, OMNI-INTEG-P, OMNI-VMW-P	OMNI-CORE-IS, OMNI-CF-P
OMNI-DB2-P, OMNI-EMC-P, OMNI-INF-P, OMNI-LOTUS-P, OMNI-OR8-P, OMNI-OV-P, OMNI-SAPDB-P, OMNI-SAP-P, OMNI-SSEA-P, OMNI-SYB-P	OMNI-INTEG-P, OMNI-CORE-IS, OMNI-CF-P

Composants	dépendent de...
OMNI-SMISA-P, OMNI-VLSAM-P	OMNI-CORE-IS, OMNI-CF-P, OMNI-PEGASUS-P

Procédure

Pour supprimer des composants logiciels Data Protector, procédez comme suit :

1. Connectez-vous en tant que `root`, puis exécutez la commande `swremove`.
2. Cliquez deux fois sur **B6960MA**, **DATA-PROTECTOR**, puis sur **OB2-CM** pour afficher une liste des composants Data Protector.
3. Sélectionnez les composants à supprimer.
4. Dans le menu **Actions**, cliquez sur **Marquer pour suppression** pour repérer les composants devant être supprimés.
5. Après avoir marqué les composants à supprimer, cliquez sur **Supprimer** dans le menu **Actions**, puis sur **OK**.

REMARQUE :

Lorsque vous marquez les composants Data Protector à supprimer et que la suppression de ceux-ci risque d'affecter le fonctionnement d'autres composants, la boîte **Dépendances** apparaît pour vous présenter la liste des composants dépendants.

Spécificités d'Oracle

Après la désinstallation de l'intégration Oracle Data Protector sur un système de serveur Oracle, le logiciel Oracle Server reste lié à la bibliothèque de base de données Data Protector. Vous devez supprimer ce lien, faute de quoi vous ne pourrez pas démarrer le serveur Oracle après suppression de l'intégration. Reportez-vous à la section "Utilisation d'Oracle après le retrait de l'intégration d'Oracle dans Data Protector" dans le *Guide d'intégration HP Data Protector*.

Sur les systèmes Solaris

Vous pouvez ajouter de nouveaux composants à l'aide de la fonctionnalité Serveur d'installation. Sur les systèmes Solaris, certains composants logiciels Data Protector dépendent les uns des autres et ne pourront fonctionner correctement si vous supprimez

l'un d'entre eux. Le tableau ci-dessous présente les composants et leurs interdépendances :

Tableau 9 Dépendances des composants logiciels Data Protector sous Solaris

Composants	Dépendant de...
Gestionnaire de cellule	
OB2-CC, OB2-DA, OB2-MA, OB2-JAVAGUI, OB2-DOCS	OB2-CORE
OB2-CS	OB2-CORE, OB2-CC
Serveur d'installation	
OB2-C-IS	OB2-CORE
OB2-CF-P	OB2-C-IS
OB2-CCP, OB2-JGUIP, OB2-DAP, OB2-MAP, OB2-NDMPP, OB2-AUTODRP, OB2-DOCSP, OB2-CHSP, OB2-FRAP, OB2-JPNP, OB2-INTGP, OB2-VMWP	OB2-C-IS, OB2-CF-P
OB2-DB2P OB2-EMCP OB2-INFP OB2-LOTP OB2-OR8P OB2-OVP OB2-SAPDP OB2-SAPP OB2-SSEAP OB2-SYBP	OB2-INTGP, OB2-C-IS, OB2-CF-P
OB2-SMISP OB2-VLSAMP	OB2-C-IS, OB2-CF-P, OB2-PEG-P

Sur les systèmes Linux

Vous pouvez ajouter de nouveaux composants à l'aide de la fonctionnalité Serveur d'installation. Sur les systèmes Linux, 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 10 Dépendances des composants logiciels Data Protector sous Linux

Composants	Dépendant de...
Gestionnaire de cellule	

Composants	Dépendant de...
OB2-CC, OB2-DA, OB2-MA, OB2-JAVAGUI, OB2-DOCS	OB2-CORE
OB2-CS	OB2-CORE, OB2-CC
Serveur d'installation	
OB2-CORE-IS	OB2-CORE
OB2-CF-P	OB2-CORE-IS
OB2-CCP, OB2-JGUIP, OB2-DAP, OB2-MAP, OB2-NDMPP, OB2-AUTODRP, OB2-DOCSP, OB2-CHSP, OB2-FRAP, OB2-JPNP, OB2-INTEGP, OB2-VMWP	OB2-CORE-IS, OB2-CF-P
OB2-DB2P OB2-EMCP OB2-INFP OB2-LOTP OB2-OR8P OB2-OVP OB2-SAPDP OB2-SAPP OB2-SSEAP OB2-SYBP	OB2-INTEGP, OB2-CORE-IS, OB2-CF-P
OB2-SMISP OB2-VLSAMP	OB2-CORE-IS, OB2-CF-P, OB2-PEG-P

Procédure

Pour supprimer des composants logiciels Data Protector sur des systèmes Linux, procédez comme suit :

1. Veillez à terminer toutes les sessions de Data Protector et à quitter l'interface utilisateur.
2. Entrez la commande `rpm | grep OB2` pour répertorier tous les packages Data Protector installés.
3. Supprimez, dans l'ordre inverse de celui où ils ont été installés, les packages indiqués dans l'Étape 2 à la page 272 à l'aide de la commande `rpm -e` *`nom du package`* et suivez les instructions qui apparaissent sur la ligne de commande.

Autres systèmes UNIX

Lorsque vous supprimez manuellement des composants d'un client Data Protector sur un système UNIX autre que Solaris ou HP-UX, mettez à jour le fichier `omni_info` dans `/usr/omni/bin/install/omni_info`.

Pour chacun des composants désinstallés, supprimez la chaîne de version du composant associé dans le fichier `omni_info`.

Si vous supprimez simplement des composants d'un client Data Protector et que vous n'avez pas exporté le client à partir de la cellule, vous devrez mettre à jour la configuration de la cellule dans le fichier `cell_info` (sur le Gestionnaire de cellule). Pour ce faire, utilisez la commande suivante sur un système dans la cellule, avec la console de cellule installée :

```
/opt/omni/bin/omnicc -update_host nom_hôte
```

4 Mise à niveau vers Data Protector 6.20

Dans ce 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 6.20, tenez compte des éléments suivants :

- Pour plus d'informations sur les plates-formes et les versions prises en charge ou non, consultez les dernières matrices de support à l'adresse http://www.hp.com/support/manuals.
- Après la mise à niveau, le Gestionnaire de cellule et le Serveur d'installation doivent avoir la même version de Data Protector installée. Bien que des versions plus anciennes des agents de disque et de support Data Protector soient prises en charge dans la même cellule, il est vivement recommandé d'installer le même version des composants Data Protector sur les clients.

  Pour connaître les limitations imposées par les anciennes versions des agents de disque et de support après une mise à niveau, consultez les *Références, notes de publication et annonces produits HP Data Protector*.
- 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.06.00, Data Protector A.06.10 ou Data Protector A.06.11, elle peut être utilisée avec Data Protector 6.20.

  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 d'informations sur l'attribution des licences, reportez-vous au Chapitre 5 à la page 327.

Condition préalable

- Réalisez une sauvegarde du système de Gestionnaire de cellule existant et de la base de données interne (IDB).
- Lorsque vous mettez à niveau le Gestionnaire de cellule à partir d'un système équipé de Data Protector A.06.00, Data Protector A.06.10 ou Data Protector A.06.11 vers un système équipé de Data Protector 6.20, vous devez au préalable mettre à niveau le Gestionnaire de cellule existant vers Data Protector 6.20.

Limites

- La mise à niveau de Data Protector 6.20 est prise en charge uniquement pour Data Protector A.06.00, Data Protector A.06.10, Data Protector A.06.11 et Application Recovery Manager A.06.00.
- Avec Data Protector 6.20, 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 6.20 de Data Protector. Les mises à niveau sont prises en charge uniquement sur une même plate-forme de Gestionnaire de cellule (de HP-UX à HP-UX, de Solaris à Solaris etde Windows à Windows).
- Si vous effectuez la mise à niveau vers Data Protector 6.20 sous Windows et si votre version de Microsoft Installer est antérieure à 2.0, le programme d'installation de Data Protector met automatiquement cette dernière à niveau vers la version 2.0. Dans ce cas, Data Protector affichera une remarque à la fin de l'installation, indiquant que MSI a été mis à niveau. Si MSI a été mis à niveau, il est vivement recommandé de redémarrer le système. Consultez le support de Microsoft pour en savoir plus sur les prérequis de MSI 2.0 en fonction des différents systèmes d'exploitation Windows.

  Pour connaître la version de MSI installée sur votre système, cliquez avec le bouton droit sur `c:\winnt\system32\msi.dll` dans l'Explorateur et sélectionnez **Propriétés**. Dans la boîte de dialogue Propriétés, sélectionnez **Version**.

Séquence de mise à niveau

Pour mettre à niveau votre cellule des versions précédentes du produit vers Data Protector 6.20, procédez comme suit :

1. Mettez à niveau le Gestionnaire de cellule et le Serveur d'installation vers Data Protector 6.20. 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.
2. Mettez à niveau les clients de l'interface utilisateur graphique.
3. Mettez à niveau les clients qui ont une intégration d'application en ligne installée, telles qu'Oracle, SAP R/3, Informix Server, Microsoft SQL Server, Microsoft Exchange Server et autres.
4. Mettez à niveau les clients sur lesquels un Agent de support (MA) est installé. Vous pouvez effectuer des sauvegardes dès que l'Agent de support (MA) est mis à niveau sur tous les clients MA de la même plate-forme que le Gestionnaire de cellule.
5. Il est recommandé de réaliser une mise à niveau des clients sur lesquels l'Agent de disque (DA) du système de fichiers est installé, dans un délai de quinze jours.

Mise à niveau dans un environnement MoM

Pour mettre à niveau votre environnement MoM vers Data Protector 6.20, 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 6.20 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.

Auto-migration des clés de cryptage

Après la mise à niveau du Gestionnaire de cellule, du Serveur d'installation et de tous les clients vers Data Protector 6.20, la commande `omnikeymigrate` migre automatiquement tous les fichiers de `banque de clés` existants à partir de tous les systèmes clients dans la cellule et les importe dans le fichier de `banque de clés` central dans le Gestionnaire de cellule Data Protector 6.20. Si une clé de cryptage active est migrée du système client spécifié, toutes les spécifications de

sauvegarde associées à ce système sont migrées automatiquement avec la clé. Une fois l'importation terminée, toutes les clés de cryptage migrées sont inactives.

Si, pour une raison quelconque, l'auto-migration ne fonctionne pas, vous pouvez migrer manuellement les clés de cryptage. Pour plus d'informations, reportez-vous à la page `omnikeymigrate` du manuel ou au *Guide de référence de l'interface de ligne de commande HP Data Protector*.

Mise à niveau à partir de Data Protector A.06.00, A.06.10 et A.06.11

Les versions A.06.00, A.06.10 et A.06.11 de Data Protector peuvent être directement mises à niveau vers Data Protector 6.20 pour les plates-formes UNIX et Windows.

Licences

Les licences existantes de Data Protector A.06.00, A.06.10 et A.06.11 sont totalement compatibles et valides pour une utilisation avec Data Protector 6.20. Pour plus d'informations sur l'attribution des licences, reportez-vous au Chapitre 5 à la page 327.

Avant de commencer

Avant de commencer la mise à niveau, reportez-vous à la section “Présentation de la mise à niveau” à la page 275 pour plus d'informations sur les limites et la séquence de mise à niveau.

Mise à niveau du Gestionnaire de cellule et du Serveur d'installation UNIX

Conditions préalables

- Arrêtez tous les services Data Protector en exécutant la commande `/opt/omni/sbin/omnisv -stop`.
- Sur Solaris, si des anciens correctifs sont installés, désinstallez-les avant la mise à niveau.
- Le shell POSIX (`sh`) doit être installé.
- Vous devez bénéficier des droits `root` pour effectuer la mise à niveau.

Si le Serveur d'installation HP-UX, Solaris ou Linux est installé conjointement avec le Gestionnaire de cellule, il est mis à niveau automatiquement lorsque la commande `omnisetup.sh` est exécutée.

Si le Serveur d'installation HP-UX, Solaris ou Linux est installé sur un système distinct, reportez-vous à la section "Mise à niveau d'un Serveur d'installation" à la page 283.

Mise à niveau d'un Gestionnaire de cellule

Le Gestionnaire de cellule HP-UX, Solaris ou Linux est mis à niveau automatiquement lorsque la commande `omnisetup.sh` est exécutée.

Sous HP-UX, cette commande met automatiquement à niveau le package existant à l'aide de l'utilitaire `swinstall`. Sous Solaris, cette commande supprime l'ensemble des packages existants à l'aide de l'utilitaire `pkgrm` et installe les nouveaux packages à l'aide de l'utilitaire `pkgadd`. Sous Linux, cette commande met automatiquement à niveau le package existant à l'aide de l'utilitaire `rpm`.

Si le Serveur d'installation est installé avec des composants client, il sera supprimé par la commande `omnisetup.sh`. Dans ce cas, installez un nouveau dépôt du Serveur d'installation au moyen de la commande `omnisetup.sh -IS`, puis réimportez le Serveur d'installation mis à niveau. Pour plus de détails, reportez-vous à la section "Importation d'un serveur d'installation dans une cellule " à la page 224.

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 317.

Définition des paramètres de noyau

Sous HP-UX, il est recommandé de régler le paramètre de noyau `maxdsiz` (taille maximale des segments de données) ou `maxdsiz_64` (pour les systèmes 64 bits) sur au moins 134 217 728 octets (128 Mo), et le paramètre de noyau `semmnu` (nombre de structures Undo de sémaphore) sur au moins 256 Mo. Une fois ces modifications effectuées, recompilez le noyau et redémarrez la machine.

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

Procédez comme suit pour mettre à niveau le Gestionnaire de cellule HP-UX, Solaris ou Linux vers Data Protector 6.20 :

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`	HP-UX sur systèmes IA-64 et PA-RISC
`solaris`	Systèmes Solaris
`linux`	Systèmes Linux

   - Copiez l'ensemble du DVD-ROM sur votre disque local :

     ```
     cp -r /dvdrom rép_image_dvd
     ```

2. Exécutez la commande `omnisetup.sh`.

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

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

   Pour lancer l'installation à partir du disque :

   - Si vous avez copié les répertoires `DP_DEPOT`, `LOCAL_INSTALL` et `AUTOPASS` sur votre disque local sous *`répertoire`*, allez sur le répertoire qui contient le fichier `omnisetup.sh` et exécutez la commande suivante :

     ```
     cd répertoire/LOCAL_INSTALL
     ./omnisetup.sh
     ```

   - Si vous avez copié l'intégralité du DVD-ROM dans *`rép_image_dvd`*, exécutez la commande `omnisetup.sh` sans paramètres :

     ```
     cd rép_image_dvd/LOCAL_INSTALL
     ./omnisetup.sh
     ```

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

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

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

   Lorsque la version A.06.00, A.06.10 ou A.06.11 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 l'installation, reportez-vous aux sections “Installation d'un Gestionnaire de cellule UNIX” à la page 45 et “Installation des Serveurs d'installation pour UNIX” à la page 64.

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` dans le répertoire `point_de_montage/LOCAL_INSTALL` sur le

DVD-ROM ou la *Guide de référence de l'interface de ligne de commande HP Data Protector*, 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 289.
- Vous devez ajuster manuellement la capacité (`VTLCAPACITY`) d'une bibliothèque de bandes virtuelle qui a été créée avec une version précédente de Data Protector et qui est définie par défaut sur 1 To après la mise à jour à Data Protector 6.20. Reportez-vous à la section "Vérification des changements de configuration" à la page 289.
- Sous HP-UX 11.23 et 11.31 (Itanium) et sous SuSE Linux (x86-64), la taille maximale des fichiers de base de données peut dépasser la taille maximale par défaut de 2 Go. Par conséquent, lors d'une mise à niveau vers Data Protector 6.20, un message d'avertissement s'affiche pour inviter à régler la taille maximale des fichiers de base de données. Vous devez effectuer cette opération après la mise à niveau, car elle peut prendre beaucoup de temps, selon la taille de la base de données. Reportez-vous à la section "Résolution des problèmes de la mise à niveau" à la page 378.

Mise à niveau d'un Serveur d'installation

Le Serveur d'installation HP-UX, Solaris ou Linux est mis à niveau automatiquement lorsque la commande `omnisetup.sh` est exécutée.

Sous HP-UX, cette commande met automatiquement à niveau le package existant à l'aide de l'utilitaire `swinstall`. Sous Solaris, cette commande supprime l'ensemble des packages existants à l'aide de l'utilitaire `pkgrm` et installe les nouveaux packages à l'aide de l'utilitaire `pkgadd`. Sous Linux, cette commande met automatiquement à niveau le package existant à l'aide de l'utilitaire `rpm`.

Si le Serveur d'installation est installé avec des composants client, il sera supprimé par la commande `omnisetup.sh`. Dans ce cas, installez un nouveau dépôt du Serveur d'installation au moyen de la commande `omnisetup.sh -IS`, puis réimportez le Serveur d'installation mis à niveau. Pour plus de détails, reportez-vous à la section "Importation d'un serveur d'installation dans une cellule " à la page 224.

IMPORTANT :

Vous ne pouvez pas mettre à niveau le Serveur d'installation si vous n'avez pas au préalable mis à niveau le Gestionnaire de cellule.

Procédure de mise à niveau

Procédez comme suit pour mettre à niveau le Serveur d'installation HP-UX, Solaris ou Linux vers Data Protector 6.20 :

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

   Par exemple :

   ```
   mkdir /dvdrom mount /dev/c0d0t0 /dvdrom
   ```

   Si vous souhaitez installer Data Protector depuis un dépôt sur le disque, procédez comme suit :

   - Pour copier les répertoires `DP_DEPOT` et `LOCAL_INSTALL` (où se trouvent les fichiers d'installation) sur votre disque local, procédez comme suit :

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

     Où *`rép_platform`* dépend du système d'exploitation et de la plate-forme du processeur sur lesquels vous mettez à niveau Data Protector:

`hpux_ia`	HP-UX sur systèmes IA-64
`hpux_pa`	HP-UX sur systèmes PA-RISC
`solaris`	Systèmes Solaris
`linux`	Systèmes Linux

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

     `cp -r /dvdrom` *`rép_image_dvd`*

2. Exécutez la commande `omnisetup.sh`.

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

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

   Pour lancer l'installation à partir du disque, effectuez l'une des étapes suivantes :

   - Si vous avez copié les répertoires `DP_DEPOT` et `LOCAL_INSTALL` sur votre disque local sous *`répertoire`*, allez sur le répertoire qui contient le fichier `omnisetup.sh` et exécutez la commande suivante :

     ```
     cd répertoire/LOCAL_INSTALL ./omnisetup.sh
     ```

   - Si vous avez copié l'intégralité du DVD-ROM dans *`rép_image_dvd`*, exécutez la commande `omnisetup.sh` sans paramètres :

     ```
     cd rép_dvd_image/LOCAL_INSTALL ./omnisetup.sh
     ```

Dès que la procédure est terminée, vous pouvez utiliser les fonctionnalités de Data Protector.

Pour obtenir la description de la commande `omnisetup.sh`, consultez le fichier `LISEZMOI` dans le répertoire `point_de_montage/LOCAL_INSTALL` sur le DVD-ROM ou la *Guide de référence de l'interface de ligne de commande HP Data Protector*, 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 289.

Mise à niveau du Gestionnaire de cellule et du Serveur d'installation Windows

Lorsque la version précédente de Data Protector est détectée, le jeu de composants pris en compte par le système d'exploitation est le même que celui qui est installé (sans les composants obsolètes). Le jeu de packages existant est supprimé et le nouveau jeu de packages est installé comme s'il s'agissait d'une nouvelle installation (propre).

Le Serveur d'installation Windows est mis à niveau automatiquement pendant la procédure de mise à niveau s'il est installé sur le même système que le Gestionnaire de cellule. L'ancien dépôt du Serveur d'installation est supprimé et, si le composant `Serveur d'installation` est sélectionné pendant l'installation, le nouveau dépôt du Serveur d'installation est copié à sa place.

Si le Serveur d'installation est installé parallèlement au client Data Protector, et si ce client est mis à niveau à distance (à l'aide de l'interface utilisateur graphique de Data Protector), le Serveur d'installation est lui aussi mis à niveau.

IMPORTANT :

Réimportez le Serveur d'installation mis à niveau une fois la procédure d'installation terminée. Pour plus de détails, reportez-vous à la section "Importation d'un serveur d'installation dans une cellule " à la page 224.

Microsoft Cluster Server

La procédure de mise à niveau du Gestionnaire de cellule fonctionnant dans un environnement Microsoft Cluster Server est différente de celle d'un Gestionnaire de cellule non configuré pour être utilisé avec Microsoft Cluster Server. La procédure détaillée correspondante est décrite à la section "Mise à niveau du Gestionnaire de cellule configuré sur Microsoft Cluster Server" à la page 322.

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 6.20 :

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. *Si Data Protector détecte le pare-feu Windows sur votre système*, la page Configuration du pare-feu Windows apparaît. Le programme d'installation de Data Protector y enregistre 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.

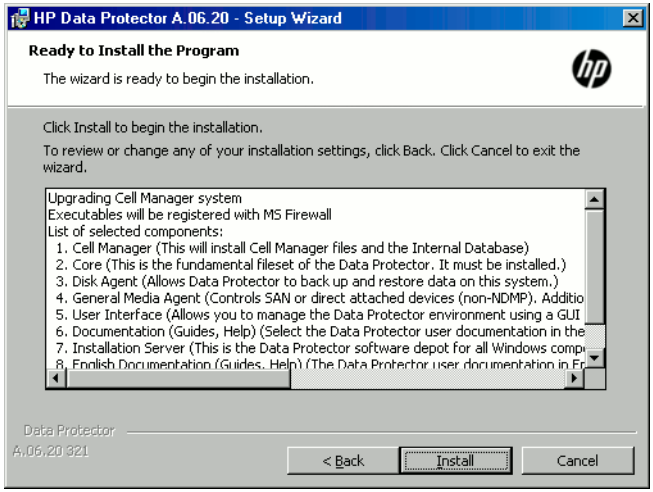


Figure 42 Page de résumé des composants sélectionnés

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

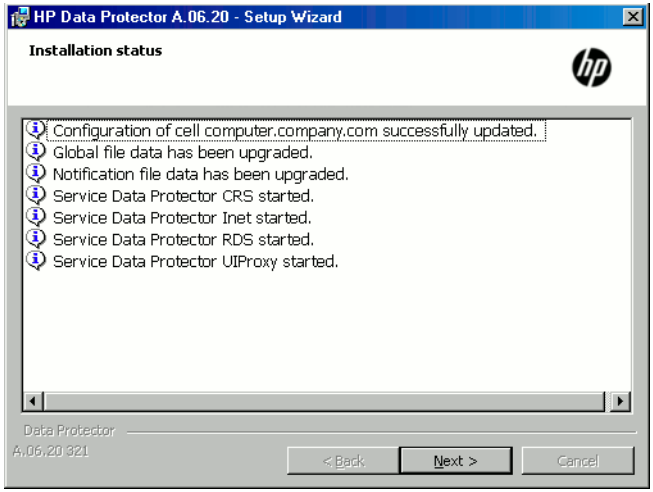


Figure 43 Page d'état de l'installation

6. Cette étape est effectuée uniquement pour une mise à niveau du Gestionnaire de cellule. Si le Serveur d'installation est installé sur un client autre que le Gestionnaire de cellule mis à niveau, cette étape n'apparaît pas.

   L'assistant d'installation vous permet d'installer ou de mettre à niveau l'utilitaire HP AutoPass si vous souhaitez télécharger et installer les mots de passe correspondant aux licences achetées directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire AutoPass, reportez-vous à la section "Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass" à la page 348.

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

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

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

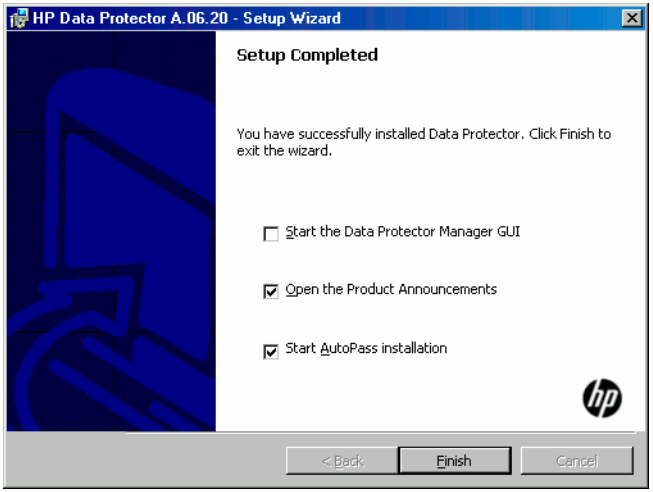


Figure 44 Sélection d'AutoPass pour l'installation

7. Cliquez sur **Terminer**.

Dès que la procédure est terminée, vous pouvez utiliser les fonctionnalités de Data Protector.

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 289.
- Vous devez ajuster manuellement la capacité (VTLCAPACITY) d'une bibliothèque de bandes virtuelle qui a été créée avec une version précédente de Data Protector et qui est définie par défaut sur 1 To après la mise à jour à Data Protector 6.20. Reportez-vous à la section "Vérification des changements de configuration" à la page 289.

Vérification des changements de configuration

Fichier d'options globales

Pendant la mise à niveau, le contenu de l'*ancien* fichier d'options globales, qui se trouve dans le répertoire /etc/opt/omni/server/options sur le Gestionnaire de cellule UNIX ou dans le répertoire `répertoire_Data_Protector\Config\server\Options` sous directory sur le Gestionnaire de cellule Windows, est fusionné avec le contenu du *nouveau* fichier d'options globales (par défaut) sur le Gestionnaire de cellule :

- `/opt/omni/newconfig/etc/opt/omni/server/options` - Gestionnaire de cellule UNIX
- `répertoire_Data_Protector\NewConfig\Server\Options` - Gestionnaire de cellule Windows

Le fichier *fusionné*, nommé `global`, se trouve dans le même répertoire que l'ancien, dans le répertoire /etc/opt/omni/server/options sur le Gestionnaire de cellule UNIX, ou dans le répertoire `répertoire_Data_Protector\Config\server\Options` sur le Gestionnaire de cellule Windows, et est utilisé par la version mise à niveau du produit. L'*ancien* fichier d'options globales est renommé en `global.1`, `global.2`, etc., selon le nombre de mises à niveau réalisées.

Les faits suivants s'appliquent après la création du fichier fusionné :

- Les variables du fichier d'options globales qui étaient actives (non mises en commentaires) dans l'ancien fichier restent actives dans le fichier fusionné. Le commentaire suivant, indiquant que la valeur de la variable a été copiée à partir de l'ancien fichier, est ajouté au fichier fusionné :

```
variable=value # Data Protector 6.20
# This value was automatically copied from previous version.
```

- Les variables du fichier d'options globale qui ne sont plus utilisées sont mises en commentaires (rendues inactives) dans le fichier fusionné ; le commentaire suivant, qui indique que la variable n'est plus utilisée, est ajouté :

  ```
  #variable=value
  # Data Protector 6.20
  # This value is no longer in use.
  ```

- Les variables dont les valeurs ne sont plus prises en charge sont mises en commentaire (rendues inactives) dans le fichier fusionné. Le commentaire suivant, contenant un modèle (*modèle_variable*) et indiquant la valeur précédente de la variable, est inséré :

  ```
  # variable=variable_template# Data Protector 6.20
  # This variable cannot be transferred automatically.
  # The previous setting was:
  # variable=valeur
  ```

- Les commentaires ne sont pas transférés dans le nouveau fichier fusionné.

Sur les systèmes Windows, le fichier d'options globales est au format Unicode et peut être modifié avec le Bloc-notes, par exemple. Après avoir modifié ce fichier, veillez à l'enregistrer au format Unicode.

La description des nouvelles options figure dans le fichier d'options globales fusionné : /etc/opt/omni/server/options/global sur un Gestionnaire de cellule UNIX et *répertoire_Data_Protector*`\Config\server\options\global` sur un Gestionnaire de cellule Windows. Pour plus d'informations sur les options globales, reportez-vous au *Guide de dépannage HP Data Protector*.

Procédure manuelle

La liste ci-dessous récapitule les étapes à réaliser manuellement une fois que la procédure de mise à niveau est terminée :

- `Omnirc` fichier

  Après la mise à niveau des systèmes du Gestionnaire de cellule et du Serveur d'installation, vous souhaitez peut-être modifier le fichier `omnirc`. Pour obtenir des informations sur la procédure à suivre, reportez-vous à la section relative à l'utilisation du fichier Omnirc dans le *Guide de dépannage HP Data Protector*.

- Ligne de commande

  Pour obtenir la liste des commandes qui ont été modifiées ou fournies avec des fonctionnalités étendues, reportez-vous à l'Annexe D à la page 471 . Vous devez vérifier et modifier les scripts utilisant les anciennes commandes. Pour les synopsis

d'utilisation, reportez-vous au *Guide de référence de l'interface de ligne de commande HP Data Protector* ou aux pages correspondantes du manuel.

- Taille maximale par défaut par répertoire DCBF

  Les paramètres par défaut des répertoires DCBF existants ne sont pas modifiés après une mise à niveau. Seuls les nouveaux répertoires créés auront une taille maximale par de défaut de 16 Go. Lorsque vous augmentez la taille maximale par défaut, vous devez également modifier l'espace disque libre pour un fichier binaire DCBF (10 à 15 % de la taille maximale recommandés). Pour modifier manuellement la taille maximale du répertoire DC, exécutez la commande suivante :

  `omnidbutil -modify_dcdir` *`répertoire`* `-maxsize` *`tailleenMo`* `-spacelow` *`tailleenMo`*

  Vous devez modifier les paramètres lorsque vous utilisez des unités de grande capacité (de type LTO 4, par exemple) et que vous sauvegardez plus de 10 millions de fichiers sur bande. En outre, vérifiez que le système de fichiers où résident les répertoires DC prennent en charge les fichiers volumineux.

- Assurez-vous que le fichier `hosts` contient les noms de domaine complets (FQDN) au format `ordinateur.entreprise.com`. Si ce n'est pas le cas, configurez le fichier de l'hôte avec le nom de domaine complet (FQDN). L'emplacement du fichier diffère en fonction du système d'exploitation.

  Systèmes Windows : `%SystemRoot%\system32\drivers\etc\`

  Systèmes UNIX : `/etc/hosts`

- Attribution de licences de sauvegarde avancée sur disque

  La capacité (`VTLCAPACITY`) d'une bibliothèque de bandes virtuelle qui a été créée avec une version précédente de Data Protector est définie par défaut sur 1 To après la mise à jour à Data Protector 6.20. En conséquence, vous devez entrer manuellement la valeur de capacité estimée de la bibliothèque par l'intermédiaire de l'interface utilisateur graphique ou de l'interface de ligne de commande.

Exemple

Avant la mise à niveau à Data Protector 6.20, les informations sur une bibliothèque de bandes virtuelle configurée nommée "VTL" ont l'aspect suivant :

```
#omnidownload -library VTL
NAME "VTL"
DESCRIPTION ""
HOST ordinateur.entreprise.com
```

```
POLICY SCSI-II
TYPE DDS
REPOSITORY
"Référentiel SCSI"
MGMTCONSOLEURL ""
```

Après la mise à niveau à Data Protector 6.20, la chaîne VTLCAPACITY est ajoutée et la capacité de la bibliothèque est définie par défaut sur 1 To.

```
#omnidownload -library VTL
NAME "VTL"
DESCRIPTION ""
HOST ordinateur.entreprise.com
POLICY SCSI-II
TYPE DDS
LIBVIRTUAL VTLCAPACITY 1
IOCTLSERIAL ""
CONTROL "Adresse SCSI"
REPOSITORY
"Référentiel SCSI"
MGMTCONSOLEURL ""
```

Pour modifier la capacité (VTLCAPACITY) d'une bibliothèque de bandes virtuelle nommée "VTL" dans un fichier ASCII nommé "libVTL.txt" dans le répertoire "C:\Temp", exécutez la commande suivante :

```
omnidownload -library VTL -file C:\Temp\libVTL.txt
```

Entrez la capacité estimée de la bibliothèque, par exemple 163 et exécutez la commande suivante :

```
omniupload -modify_library VTL -file C:\Temp\libVTL.txt
```

REMARQUE :

La valeur de consommation de capacité estimée de la bibliothèque virtuelle (VTLCAPACITY) en téra-octets (To) doit être un nombre entier, de manière à empêcher l'apparition d'erreurs de capacité non valide.

Pour vérifier la configuration de la bibliothèque, exécutez la commande suivante :

```
omnidownload -library VTL
```

```
#omnidownload -library VTL
NAME "VTL"
DESCRIPTION ""
HOST ordinateur.entreprise.com
POLICY SCSI-II
TYPE DDS
LIBVIRTUAL VTLCAPACITY 163
IOCTLSERIAL ""
CONTROL "Adresse SCSI"
REPOSITORY
"Référentiel SCSI"
MGMTCONSOLEURL ""
```

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 293.

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 275.

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 83. 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 92.

Pour mettre à niveau les clients UNIX en local, reportez-vous à la section “Installation en local de clients UNIX et Mac OS X” à la page 151.

Limite

Si vous effectuez la mise à niveau vers Data Protector 6.20 sous Windows, HP-UX et Linux, la base de données de sauvegarde incrémentale avancée ne peut pas être mise à niveau vers la nouvelle version. L'ancien référentiel de sauvegarde incrémentale avancée est supprimé du répertoire `répertoire_Data_Protector\enhincrdb\point_de_montage`. Lors de la première sauvegarde complète après la mise à niveau du client, un nouveau référentiel est créé au même emplacement. Notez que la première sauvegarde après la mise à niveau doit être complète.

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. Reportez-vous à la section “Installation en local de clients Novell NetWare” à la page 134 pour plus de détails.

Clients Linux

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, supprimez le fichier et réalisez une mise à niveau à distance des composants logiciels Data Protector à partir de l'interface utilisateur graphique 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. Pour conserver vos modifications, créez une copie de sauvegarde au préalable et transférez les paramètres manuellement vers le nouveau fichier après la mise à niveau.

Mise à niveau du client configuré sur MC/ServiceGuard

Si vous mettez à niveau le client utilisant MC/ServiceGuard et que le composant d'intégration Data Protector à mettre à niveau est installé sur le même nœud que le Gestionnaire de cellule, mettez à niveau d'abord les nœuds physiques, puis procédez comme suit :

1. Exportez l'hôte virtuel par la commande :

   ```
   omnicc -import_host nom_hôte_virtuel
   ```

2. Réimportez l'hôte virtuel en exécutant la commande :

   ```
   omnicc -import_host nom_hôte_virtuel -virtual
   ```

Mise à niveau de clients avec des intégrations

Si vous mettez à niveau un client Data Protector sur lequel l'intégration est installée (intégration pour Oracle, SAP R/3, Microsoft Volume Shadow Copy Service ou HP StorageWorks P6000 EVA Disk Array Family, module de récupération automatique après sinistre, intégration pour Microsoft Exchange Server, Microsoft SQL Server, HP StorageWorks P9000 XP Disk Array Family ou EMC Symmetrix, etc.), procédez comme indiqué dans les paragraphes ci-dessous pour effectuer la mise à niveau :

- 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 296.
- 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 297.
- Pour obtenir des instructions sur la procédure de mise à niveau de l'intégration Microsoft Volume Shadow Copy Service, reportez-vous à la section “Mise à niveau de l'intégration Microsoft Volume Shadow Copy Service” à la page 299.
- Pour obtenir des instructions sur la procédure de mise à niveau de l'intégration HP StorageWorks P6000 EVA Disk Array Family, reportez-vous à la section “Mise à niveau de l'intégration HP StorageWorks P6000 EVA Disk Array Family” à la page 299.
- Pour obtenir des instructions sur la procédure de mise à niveau du module de récupération automatique après sinistre, reportez-vous à la section “Mise à niveau du module de récupération automatique après sinistre” à la page 300.
- Pour obtenir des instructions sur la procédure de mise à niveau de l'intégration Microsoft Exchange Server, Microsoft SQL Server, HP StorageWorks P9000 XP Disk Array Family ou EMC Symmetrix, ou d'une autre intégration, reportez-vous à la section “Mise à niveau des autres intégrations” à la page 301.

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 par l'intermédiaire d'une installation à distance de 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.

L'utilisateur root n'est plus requis

Sur les clients UNIX, l'intégration Oracle Server Data Protector ne configure plus, ne vérifie plus la configuration et n'explore plus les bases de données Oracle pour l'utilisateur `root`. Ces opérations s'exécutent sous le compte utilisateur du système d'exploitation indiqué lorsque vous définissez une spécification de sauvegarde. Par conséquent, vous pouvez sans risque supprimer l'utilisateur `root` du groupe d'utilisateurs de Data Protector.

REMARQUE :

Pour les sessions de sauvegarde ZDB et de restauration instantanée, l'utilisateur `root` reste nécessaire.

Une fois la mise à niveau effectuée, il est également recommandé de contrôler la configuration de chaque base de données Oracle. Au cours de cette vérification, Data Protector copie le compte d'utilisateur du système d'exploitation (propriétaire de sauvegarde) de la spécification de sauvegarde vers le fichier de configuration de base de données Oracle Data Protector correspondant.

Si le contrôle de configuration n'est pas effectué, le fichier de configuration ne sera pas mis à jour. Dans ce cas, au cours de la restauration, Data Protector explore les bases de données Oracle sous le propriétaire de sauvegarde de la dernière session de sauvegarde. Si une session de sauvegarde de ce type n'a pas été créée au cours des trois derniers mois, l'utilisateur `root` sera utilisé en dernier recours.

MML Data Protector

Après avoir mis à niveau un client UNIX Data Protector A.06.00, supprimez le lien symbolique renvoyant à la MML Data Protector car il n'est plus utile :

1. Accédez au répertoire `ORACLE_HOME/lib`.
2. Si le fichier `libobk.sl.orig` (`libobk.so.orig`) existe dans le répertoire `ORACLE_HOME/lib`, exécutez :

   HP–UX : `mv libobk.sl.orig libobk.sl`

   Autres systèmes UNIX : `mv libobk.so.orig libobk.so`

   où `libobk.sl.orig` (`libobk.so.orig`) est le lien programmable Oracle tel qu'il existait avant la configuration de l'intégration.

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 ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Configurations Oracle ASM utilisant HP StorageWorks P6000 EVA Disk Array Family pour le stockage des données

Pour activer la prise en charge de la création de répliques cohérentes des données Oracle Server sur P6000 EVA Array dans les configurations avec gestion de stockage automatique, vous devez mettre à niveau les composants Data Protector, l'intégration Oracle et l'Agent HP StorageWorks P6000 EVA SMI-S sur le système d'application et le système de sauvegarde.

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 par l'intermédiaire d'une installation à distance de l'agent d'intégration SAP R/3 sur le client à l'aide de l'interface graphique de Data Protector. Sous UNIX, notez que si vous mettez à niveau le client qui ne réside pas sur le Gestionnaire de cellule, il n'est pas nécessaire

de spécifier l'option `-install sap`. Dans ce cas, le programme d'installation sélectionnera sans émettre d'invite les mêmes composants que ceux déjà installés sur le système.

MML Data Protector

Après avoir mis à niveau un client Data Protector A.06.00 UNIX SAP R/3, supprimez le lien symbolique renvoyant à la MML Data Protector car il n'est plus utile. Pour plus de détails, reportez-vous à la section “MML Data Protector” à la page 297.

Sessions ZDB compatibles SAP

Selon les normes SAP, il est recommandé, lors des sessions ZDB, de démarrer BRBACKUP sur le système de sauvegarde (sessions ZDB compatibles SAP). Data Protector 6.20 permet de respecter ces normes. Configurez d'abord le système de sauvegarde selon les instructions fournies dans le guide SAP pour Oracle (sauvegarde split mirror, configuration du logiciel), puis installez le composant Data Protector SAP `R/3 Integration` sur le système de sauvegarde. Pour finir, configurez Data Protector pour des sessions ZDB compatibles SAP comme décrit dans le *Guide d'intégration ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector*.

Configuration d'une instance d'Oracle pour la restauration instantanée

Si les fichiers de contrôle, les catalogues de récupération ou les journaux de rétablissement archivés se trouvent dans le même groupe de volumes (si LVM est utilisé) ou dans le même volume source que les fichiers de base de données, vous pouvez :

- Reconfigurer l'instance Oracle.
- Définir les variables `omnirc ZDB_ORA_INCLUDE_CF_OLF, ZDB_ORA_INCLUDE_SPF et ZDB_ORA_NO_CHECKCONF_IR`.
- Configurer Data Protector pour démarrer BRBACKUP sur le système de sauvegarde (sessions ZDB compatibles SAP).

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

Mise à niveau de l'intégration Microsoft Volume Shadow Copy Service

Mise à niveau à partir de HP Data Protector A.06.00

Après la mise à niveau, les spécifications de sauvegarde VSS HP Data Protector A.06.00 ne sont plus utilisables. Toutes les spécifications de sauvegarde VSS HP Data Protector A.06.00 doivent être recréées.

Les sessions de sauvegarde pour lesquelles la restauration instantanée est activée ne pourront plus être utilisées en vue de la restauration intantanée après la mise à niveau. Avant de lancer la mise à niveau, supprimez les sessions à l'aide de la commande `omnidbvss`.

Sessions de sauvegarde avec restauration instantanée activée après la mise à niveau à partir de HP Data Protector A.06.10 ou HP Data Protector A.06.11

Une fois que vous avez mis à niveau l'intégration VSS depuis une version antérieure, vous devez résoudre les volumes sources sur le système d'application pour pouvoir effectuer des sessions de sauvegarde ZDB sur disque et ZDB sur disque + bande. Sinon, les sessions de sauvegarde ZDB sur disque échoueront et les sessions de sauvegarde ZDB sur disque + bande ne seront effectives que sur bande, les répliques n'étant pas conservées sur la baie de disques. Effectuez l'opération de résolution à partir de n'importe quel client VSS de la cellule, en procédant comme suit :

```
omnidbvss –resolve {–apphost ApplicationSystem | –all}
```

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

Mise à niveau de l'intégration HP StorageWorks P6000 EVA Disk Array Family

Eléments à prendre en considération

- Lors de la mise à niveau vers Data Protector 6.20, notez que la stratégie de snapshot *souple* pour la création de répliques sur P6000 EVA Array n'est plus prise en charge dans Data Protector version 6.20. La stratégie de snapshot *stricte* est appliquée pour toutes les sessions de sauvegarde avec temps d'indisponibilité nul dans lesquelles intervient cette baie de disques. Après la mise à niveau, lorsqu'une session de sauvegarde avec temps d'indisponibilité nul utilisant la stratégie de snapshot *souple* est exécutée, un avertissement est émis et la stratégie de snapshot *stricte* est alors appliquée, mais la spécification de sauvegarde avec temps d'indisponibilité nul proprement dite n'est pas mise à jour. Pour éviter ce

type d'avertissement, vous devez mettre à jour manuellement les spécifications de sauvegarde avec temps d'indisponibilité nul.

Pour mettre à jour une spécification de sauvegarde avec temps d'indisponibilité nul manuellement afin d'utiliser la stratégie de snapshot *stricte* désormais implicite, ouvrez la spécification de sauvegarde dans l'interface utilisateur de Data Protector, modifiez l'une des options et rétablissez-la, puis enregistrez la spécification de sauvegarde en cliquant sur **Appliquer**.

Pour plus d'informations sur les stratégies de snapshot pour la création de répliques sur P6000 EVA Array, reportez-vous au *Guide de l'administrateur ZDB (sauvegarde avec temps d'indisponibilité nul) HP Data Protector* et à l'aide en ligne.

Mise à niveau du module de récupération automatique après sinistre

Le module de récupération automatique après sinistre (récupération après sinistre automatique avancée et récupération automatique après sinistre) de Data Protector 6.20 n'est pas entièrement compatible avec la version A.06.00 du module (sans l'installation du correctif DPWIN_00270).

Le Tableau 11 à la page 300 répertorie toutes les combinaisons et les problèmes de compatibilité.

Tableau 11 Compatibilité EADR et OBDR après une mise à niveau

Version du client Data Protector		**Résultat**
Sauvegarde	**Création d'image**	
A.06.00 (sans le correctif DPWIN_00270)	A.06.00 (sans le correctif DPWIN_00270)	Création d'une image
A.06.00 (sans le correctif DPWIN_00270)	A.06.00 (avec le correctif DPWIN_00270), A.06.10, A.06.11 ou 6.20	Erreur.
A.06.00 (avec le correctif DPWIN_00270), A.06.10, A.06.11 ou 6.20	A.06.00 (sans le correctif DPWIN_00270)	Erreur.
A.06.00 (avec le correctif DPWIN_00270), A.06.10, A.06.11 ou 6.20	A.06.00 (avec le correctif DPWIN_00270), A.06.10, A.06.11 ou 6.20	Création d'une image

Pour plus d'informations sur les modifications des procédures EADR et OBDR, voir le *Guide de récupération après sinistre HP Data Protector*.

Mise à niveau des autres intégrations

Si une intégration Microsoft Exchange Server, Microsoft SQL Server, HP StorageWorks P9000 XP Disk Array Family, EMC Symmetrix ou autre est installée sur le client Data Protector, mettez ce dernier à niveau, soit localement via la commande `omnisetup.sh -install` *`liste_de_composants`* sur les systèmes UNIX ou `setup.exe` sur les systèmes Windows, soit à distance via l'interface utilisateur graphique de Data Protector. Pour obtenir la liste des codes des composants Data Protector, reportez-vous à la section "Installation en local de clients UNIX et Mac OS X" à la page 151. Notez que si vous mettez à niveau le client qui ne réside pas sur le Gestionnaire de cellule, il n'est pas nécessaire de spécifier l'option `-install` *`liste_composants`*. Dans ce cas, le programme d'installation sélectionnera sans émettre d'invite les mêmes composants que ceux déjà installés sur le système.

Mise à niveau dans un environnement MoM

Vous pouvez mettre à niveau un environnement MoM de manière séquentielle. Toutefois, gardez à l'esprit les limites suivantes :

Limites

- Vous ne pouvez pas utiliser un **format de support de fichier distribué** avec vos bibliothèques de fichiers tant que tous les Gestionnaires de cellule n'ont pas été mis à niveau vers Data Protector 6.20.

Pour mettre à niveau votre environnement MoM vers Data Protector 6.20, procédez comme suit :

1. Mettez à niveau le Gestionnaire MoM/serveur CMMDB vers Data Protector 6.20.

   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 278 et "Mise à niveau du Gestionnaire de cellule et du Serveur d'installation Windows" à la page 285.

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 utilisateur graphique du MoM Data Protector 6.20.

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 6.20 Edition serveur unique. Pour plus de détails, reportez-vous à la section "Mise à niveau des versions antérieures de l'Edition serveur unique (SSE) vers Data Protector 6.20 Edition serveur unique (SSE)" à la page 302.
- De Data Protector 6.20 Edition serveur unique vers Data Protector 6.20. Pour plus de détails, reportez-vous à la section "Mise à niveau de Data Protector 6.20 Edition serveur unique (SSE) vers Data Protector 6.20" à la page 302.

Mise à niveau des versions antérieures de l'Edition serveur unique (SSE) vers Data Protector 6.20 Edition serveur unique (SSE)

La procédure de mise à niveau des versions antérieures de SSE vers Data Protector SSE est identique à celle des versions précédentes de Data Protector vers Data Protector 6.20. Pour plus d'informations, reportez-vous à la section "Mise à niveau à partir de Data Protector A.06.00, A.06.10 et A.06.11" à la page 278.

Mise à niveau de Data Protector 6.20 Edition serveur unique (SSE) vers Data Protector 6.20

Licences

Vous devez posséder une licence pour effectuer la mise à niveau à partir de Data Protector 6.20 Edition serveur unique vers Data Protector 6.20. Pour plus d'informations sur l'attribution des licences, reportez-vous au Chapitre 5 à la page 327.

La mise à niveau de l'Edition serveur unique de Data Protector 6.20 vers Data Protector 6.20 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 303.
- 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 303.

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 6.20, reportez-vous à la section “Mise à niveau à partir de Data Protector A.06.00, A.06.10 et A.06.11” à la page 278.

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 utilisateur graphique de Data Protector et ajoutez un mot de passe permanent.

Mise à niveau de plusieurs installations

Pour mettre à niveau l'Edition serveur unique de Data Protector installée sur plusieurs systèmes, procédez comme suit :

1. Désignez parmi les systèmes où l'Edition serveur unique est installée celui qui doit devenir le nouveau Gestionnaire de cellule. Reportez-vous à la section “Choix du système Gestionnaire de cellule” à la page 38.

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 utilisateur graphique 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 252.

5. Si nécessaire, importez les supports vers le nouveau Gestionnaire de cellule.

   Réalisez cette étape si vous envisagez de fréquentes restaurations de supports créés sur les autres systèmes Edition serveur unique. Si ces restaurations sont peu probables, vous pouvez utiliser l'option `Lister depuis support`. Dans *l'index de l'aide en ligne, recherchez : "importation, supports"* pour obtenir des informations sur l'importation de supports et sur la restauration à l'aide de l'option `Lister depuis support`.

Mise à niveau à partir de HP StorageWorks Application Recovery Manager A.06.00

Présentation

Application Recovery Manager est une solution de récupération de logiciels évolutive qui fournit des sauvegardes et des restaurations automatisées de données d'applications Exchange et SQL et qui a été conçue pour améliorer la disponibilité des applications grâce à une restauration très rapide des données.

Data Protector 6.20 prend en charge la mise à niveau à partir de Application Recovery Manager A.06.00 et prend en charge toutes les fonctionnalités de Application Recovery Manager A.06.00. La configuration et la base de données internes sont conservées après la mise à niveau.

Limites

- Le changement de plate-forme du Gestionnaire de cellule n'est pas pris en charge dans la version 6.20 de Data Protector. Les mises à niveau sont prises en charge uniquement sur une même plate-forme de Gestionnaire de cellule (Windows 32 bits à Windows 32 bits, ou Windows 64 bits à Windows 64 bits).

Procédure de mise à niveau

Les procédures de mise à niveau à partir de Application Recovery Manager A.06.00 et d'anciennes versions de Data Protector vers Data Protector 6.20 sont identiques. Reportez-vous aux sections Mise à niveau du Gestionnaire de cellule et Mise à niveau des clients.

Sauvegarde de la base de données interne après la mise à niveau

Les anciennes sauvegardes de la base de données internes créées avec `dbtool.pl` ne sont pas utilisables avec Data Protector. Vous devez configurer une nouvelle spécification de sauvegarde pour sauvegarder la base de données interne et la configuration. Dans l'index de l'aide en ligne, recherchez : “IDB, configuration de sauvegardes”.

Contrairement à Application Recovery Manager, la sauvegarde de la base IDB dans Data Protector utilise un lecteur de bande et se différencie par les opérations suivantes :

- les services Data Protector ne sont pas arrêtés lors de la sauvegarde comme avec `dbtool.pl`,
- la base de données VSS n'est pas sauvegardée.

Mise à niveau de spécifications de sauvegarde

Dans Application Recovery Manager, une spécification de sauvegarde ne contient aucun lecteur de bande. Une fois la mise à niveau vers Data Protector effectuée, les spécifications de sauvegarde peuvent être utilisées uniquement pour des sauvegardes ZDB sur disque. Pour utiliser la fonctionnalité de bande (ZDB sur disque + bande, ZDB sur bande), vous devez reconfigurer les spécifications de sauvegarde, en indiquant le lecteur de bande.

Changements dans l'utilisation de la commande omnib

Si aucune option n'est spécifiée, Data Protector utilise l'option ZDB sur disque + bande par défaut. Les sessions de sauvegarde Application Recovery Manager lancées

à partir de l'interface de ligne de commande, à l'aide de la commande `omnib`, échoueront donc du fait de l'absence de lecteurs de bande. Pour conserver vos spécifications de sauvegarde existantes sans les reconfigurer pour des sauvegardes ZDB sur disque + bande, utilisez l'option `-disk_only` pour exécuter une sauvegarde ZDB sur disque.

Mise à niveau de Solaris 8 vers Solaris 9

Si l'Agent de disque (DA) Data Protector est installé sous Solaris 8 et si vous voulez mettre à niveau le système d'exploitation vers Solaris 9, prenez en compte l'impact de cette mise à niveau sur Data Protector. Il est recommandé de remplacer l'Agent de disque générique Solaris installé sur le système par l'Agent de disque Solaris 9 pour garantir le bon fonctionnement de Data Protector et activer les options de sauvegarde avancées pour Solaris 9, comme par exemple la sauvegarde d'attributs étendus.

Réalisez la mise à niveau comme suit :

1. Mettez à niveau le système d'exploitation de Solaris 8 vers Solaris 9. Pour plus d'informations, reportez-vous à la documentation Solaris.
2. Installez l'Agent de disque à distance sur le système mis à niveau à l'aide d'un Serveur d'installation. L'Agent de disque générique Solaris sera ainsi remplacé par l'Agent de disque Solaris 9. Reportez-vous à la section “Installation distante de clients Data Protector” à la page 83 ou à la page `ob2install` du manuel.

Migration de HP-UX 11.x (PA-RISC) vers HP-UX 11.23/11.31 (IA-64)

Cette section décrit la procédure à suivre pour faire migrer votre Gestionnaire de cellule d'un système HP-UX 11.x basé sur une architecture PA-RISC vers un système HP-UX 11.23/11.31 pour l'architecture Intel Itanium 2 (IA-64).

Limites

Pour plus d'informations sur les versions des systèmes d'exploitation, les plates-formes, les architectures de processeurs et les composants Data Protector pris en charge et pour connaître les correctifs requis, les limites générales et les conditions requises pour l'installation, reportez-vous aux *Références, notes de publication et annonces produits HP Data Protector*.

- La migration est uniquement prise en charge à partir du Gestionnaire de cellule Data Protector 6.20 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 310.

Condition préalable

- Avant la migration, le Gestionnaire de cellule Data Protector sur un système HP-UX 11.x basé sur une architecture PA-RISC doit être mis à niveau vers Data Protector 6.20.

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. Reportez-vous à la section "Migration de licence vers Data Protector 6.20" à la page 361 pour plus de détails.

REMARQUE :

Sur les plates-formes Gestionnaire de cellule qui ne prennent pas en charge l'interface utilisateur graphique d'origine de Data Protector, vous pouvez utiliser l'interface utilisateur graphique Java de Data Protector ou installer l'interface utilisateur graphique d'origine de Data Protector sur un système qui la prend en charge. Utilisez la commande `omniusers` pour créer un compte utilisateur distant sur le nouveau Gestionnaire de cellule. Vous pouvez alors utiliser ce compte utilisateur avec l'interface utilisateur graphique 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 99.

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 hôtes approuvés et la sécurisation des clients Data Protector, reportez-vous aux sections “Sécurisation de clients” à la page 235 et “Groupements d'hôtes approuvés” à la page 248.

3. Sauvegardez la base de données IDB. Vérifiez que le support utilisé sera accessible par la suite sur le nouveau système du Gestionnaire de cellule. 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 IA-64. Dans l'index de l'aide en ligne, recherchez "Restauration de la base de données interne".

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 253.

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 44.

7. Si vous avez modifié le port Inet Data Protector par défaut sur l'ancien Gestionnaire de cellule, définissez le même port Inet sur le nouveau Gestionnaire de cellule. Reportez-vous à la section “Modification du numéro de port par défaut de Data Protector” à la page 414.

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. Dans l'index de l'aide en ligne, recherchez "Restauration de la base de données interne".

   Si l'ancien Gestionnaire de cellule était compatible avec les clusters, commentez les variables `SHARED_DISK_ROOT` et `CS_SERVICE_HOSTNAME` dans le fichier `/etc/opt/omni/server/sg/sg.conf` . Cela est nécessaire même si le nouveau Gestionnaire de cellule est compatible avec les clusters.

9. Pour faire migrer l'IDB et les clients vers le nouveau Gestionnaire de cellule et pour reconfigurer les paramètres du Gestionnaire de cellule, procédez comme suit sur le *nouveau* Gestionnaire de cellule :

   - Si vous souhaitez configurer un Gestionnaire de cellule IA-64 autonome, exécutez la commande `omnimigrate.pl -configure`. Reportez-vous à la page `omnimigrate.pl` du manuel.
   - Si vous souhaitez configurer un Gestionnaire de cellule IA-64 compatible cluster :
     a. Exécutez la commande `omnimigrate -configure_idb` pour configurer l'IDB de l'ancien Gestionnaire de cellule pour une utilisation avec le nouveau Gestionnaire de cellule. Reportez-vous à la page `omnimigrate.pl` du manuel.
     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 `omnimigrate.pl` du manuel.
     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. Dans l'index de l'aide en ligne, recherchez l'entrée "Configuration de l'intégration de MC/ServiceGuard".
     e. Exécutez la commande `omnimigrate -configure_clients` pour faire migrer les clients de l'ancien Gestionnaire de cellule vers le nouveau Gestionnaire de cellule. Notez que l'ancien Gestionnaire de cellule conserve les clients dans les fichiers de configuration, mais il ne sera plus leur Gestionnaire de cellule.

REMARQUE :

Si le répertoire `/etc/opt/omni/server` est situé sur le volume de cluster partagé, les changements de configuration effectués par le script `omnimigrate.pl` affecteront tous les noeuds du cluster.

REMARQUE :

L'ancien Gestionnaire de cellule deviendra automatiquement un client dans la nouvelle cellule. Vous pouvez désinstaller le composant Gestionnaire de cellule de l'ancien Gestionnaire de cellule car il n'est plus nécessaire. Reportez-vous à la section “Changement de composants logiciels Data Protector” à la page 268.

10. Configurez les licences sur le nouveau Gestionnaire de cellule. Reportez-vous à la section “Structure de produit et licences de Data Protector 6.20” à la page 358.
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 utilisateur graphique 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 310.
    - 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 de type 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 311.

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 "Exportation de systèmes clients".
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 nouveaux clients MoM.

REMARQUE :

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

Détails relatifs au Serveur d'installation

La migration du Serveur d'installation ne s'effectue pas dans le cadre de la migration du Gestionnaire de cellule. Si un Serveur d'installation est installé sur votre ancien Gestionnaire de cellule, il ne migrera pas vers le nouveau Gestionnaire de cellule et restera le Serveur d'installation de votre cellule.

Si vous souhaitez également utiliser le nouveau Gestionnaire de cellule en tant que Serveur d'installation, installez le composant Serveur d'installation sur le nouveau

Gestionnaire de cellule après la migration et importez-le dans la cellule. Dans l'index de l'aide en ligne, recherchez : “Serveur d'installation”.

Migration d'un système Windows 32 bits/64 bits vers un système Windows 64 bits/Windows Server 2008

Cette section décrit la procédure de migration de votre Gestionnaire de cellule existant d'un système Windows 32 bits vers un système Windows 64 bits ou d'un système Windows 64 bits vers un système Windows Server 2008 64 bits.

Limites

Pour plus d'informations sur les versions des systèmes d'exploitation, les plates-formes, les processeurs et les éléments Data Protector pris en charge et pour connaître les correctifs requis, les limites générales et les conditions requises pour l'installation, reportez-vous aux Références, notes de publication et annonces produits HP Data Protector.

Condition préalable

- Avant la migration, le Gestionnaire de cellule de Data Protector sur un système Windows 32 bits doit être mis à niveau vers Data Protector 6.20.

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 6.20” à la page 361 pour plus de détails.

Procédure de migration

Réalisez la migration comme suit :

1. Installez un client Data Protector sur le système Windows 64 bits ou sur le système Windows Server 2008 64 bits qui deviendra votre nouveau Gestionnaire de cellule. Pour plus de détails, reportez-vous à la section “Installation de clients Windows” à la page 92.

2. Importez le système dans la cellule de l'ancien Gestionnaire de cellule.
3. Sur l'*ancien* Gestionnaire de cellule, ajoutez le nom d'hôte du nouveau Gestionnaire de cellule à la liste des hôtes approuvés sur les clients sécurisés. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez :

   ```
   perl winomnimigrate.pl -prepare_clients
   Nom_nouveau_gestionnaire
   ```

   `Nom_nouveau_gestionnaire` est le nom de client du nouveau Gestionnaire de cellule de l'étape précédente. Pour plus d'informations sur `winomnimigrate.pl`, reportez-vous au *Guide de référence de l'interface de ligne de commande HP Data Protector*.

   Pour plus d'informations sur les hôtes approuvés et la sécurisation des clients Data Protector, reportez-vous aux sections “Sécurisation de clients” à la page 235 et “Groupements d'hôtes approuvés” à la page 248.
4. Sauvegardez la base de données IDB. Vérifiez que le support utilisé sera accessible par la suite sur le nouveau système du Gestionnaire de cellule. Dans l'index de l'aide en ligne, recherchez : "sauvegarde de la base de données interne".
5. Restaurez la base IDB dans un emplacement temporaire sur le nouveau Gestionnaire de cellule. Selon l'option choisie pour la sauvegarde de la base IDB, vous devrez peut-être configurer le périphérique et importer le catalogue à partir du support approprié. Une fois l'objet de sauvegarde IDB dans la base IDB, vous pouvez restaurer l'IDB afin de déplacer les données de configuration vers le nouveau système. Dans l'index de l'aide en ligne, recherchez : "restauration de la base de données interne".
6. Désinstallez le client Data Protector du nouveau Gestionnaire de cellule. Reportez-vous à la section “Désinstallation d'un client Data Protector” à la page 253.
7. Installez le Gestionnaire de cellule Data Protector sur le nouveau Gestionnaire de cellule. Reportez-vous à la section “Installation du Gestionnaire de cellule (CM) et du Serveur d'installation (IS) de Data Protector” à la page 44.
8. Si vous avez modifié le port Inet Data Protector par défaut sur l'ancien Gestionnaire de cellule, définissez le même port Inet sur le nouveau Gestionnaire de cellule. Reportez-vous à la section “Modification du numéro de port par défaut de Data Protector” à la page 414.

9. Déplacez la base de données IDB restaurée (résidant dans un emplacement temporaire sur le nouveau Gestionnaire de cellule) et les données de configuration sur le nouveau Gestionnaire de cellule, dans le même emplacement qu'elles occupaient sur l'ancien Gestionnaire de cellule. Ne redémarrez pas les services Data Protector. Dans l'index de l'aide en ligne, recherchez : "restauration de la base de données interne".

REMARQUE :

Lors de la mise à niveau à partir d'un système Windows 32 bits/64 bits vers un système Windows 64 bits/Windows Server 2008, les fichiers IDB sont replacés dans le nouvel emplacement par défaut. Vous devez donc vérifier que les fichiers IDB se trouvent dans le même répertoire qu'avant la migration, sous *répertoire_Data_Protector* et non *données_programme_Data_Protector*.

10. Pour faire migrer l'IDB et les clients vers le nouveau Gestionnaire de cellule et pour reconfigurer les paramètres du Gestionnaire de cellule, procédez comme suit sur le *nouveau* Gestionnaire de cellule :

    - Configurez un Gestionnaire de cellule autonome. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez :

      ```
      perl winomnimigrate.pl -configure
      ```

      Si vous migrez le Gestionnaire de cellule vers un système Windows Server 2008 64 bits, vous pouvez utiliser l'option `-keep_dcdirs` pour conserver sans condition les références à d'autres répertoires DCBF dans l'IDB migrée :

      ```
      perl winomnimigrate.pl -configure -keep_dcdirs
      ```

    - Pour configurer un Gestionnaire de cellule compatible cluster :

      a. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez `perl winomnimigrate.pl -configure_idb` afin de configurer la base de données IDB de l'ancien Gestionnaire de cellule en vue d'une utilisation sur le nouveau Gestionnaire de cellule.

      Si vous migrez le Gestionnaire de cellule vers un système Windows Server 2008 64 bits, vous pouvez utiliser l'option `-keep_dcdirs` pour conserver sans condition les références à d'autres répertoires DCBF dans l'IDB migrée : `perl winomnimigrate.pl -configure_idb -keep_dcdirs`

      b. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez `perl winomnimigrate.pl -configure_cm` afin de reconfigurer les données de configuration transférées de l'ancien Gestionnaire de cellule en vue d'une utilisation sur le nouveau Gestionnaire de cellule.

      c. Exportez l'ancien serveur virtuel de la cellule en exécutant la commande `omnicc -export_host` *`Nom_ancien_gestionnaire`*.

      d. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez `perl winomnimigrate.pl -configure_clients` pour migrer les clients de l'ancien Gestionnaire de cellule vers le nouveau Gestionnaire de cellule. Notez que l'ancien Gestionnaire de cellule conserve les clients dans les fichiers de configuration, mais il ne sera plus leur Gestionnaire de cellule.

REMARQUE :

L'ancien Gestionnaire de cellule deviendra automatiquement un client dans la nouvelle cellule. Vous pouvez désinstaller le composant Gestionnaire de cellule de l'ancien Gestionnaire de cellule car il n'est plus nécessaire. Reportez-vous à la section “Changement de composants logiciels Data Protector” à la page 268.

11. Si vous avez installé le nouveau Gestionnaire de cellule 64 bits dans un autre répertoire que celui où l'ancien Gestionnaire de cellule était installé, les liens internes dans la base IDB seront ajoutés dans les chemins de l'ancien Gestionnaire de cellule. Ajoutez manuellement les nouveaux chemins des répertoires du catalogue de détails sur le nouveau Gestionnaire de cellule à l'aide de l'interface utilisateur graphique de Data Protector. Dans l'index de l'aide en ligne, recherchez : "création de répertoires DC".
12. Configurez les licences sur le nouveau Gestionnaire de cellule. Reportez-vous à la section “Structure de produit et licences de Data Protector 6.20” à la page 358.
13. Des étapes supplémentaires sont nécessaires dans les cas suivants :
    - Votre cellule fait partie d'un environnement MoM. Reportez-vous à la section “Informations spécifiques à MoM” à la page 316.
    - 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 317.

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 6.20 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.06.00, A.06.10 ou A.06.11 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 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 6.20. Reportez-vous à la section "Mise à niveau du Gestionnaire de cellule et du Serveur d'installation UNIX" à la page 278.

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 6.20. Suivez les étapes de la procédure décrite à la section "Mise à niveau du Gestionnaire de cellule et du Serveur d'installation UNIX" à la page 278.

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_DP55.sh` et `mafailover_DP55.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.

5. Arrêtez les services Data Protector s'ils sont en cours d'exécution :

   ```
   /opt/omni/sbin/omnisv -stop
   ```

6. Démontez le disque partagé :

   ```
   umount disque_partagé
   ```

7. Désactivez le groupe de volumes :

   ```
   vgchange -a n nom_gv
   ```

Nœud principal

Reconnectez-vous au nœud principal et procédez comme suit :

1. Redémarrez le package Data Protector :

   ```
   cmrunpkg nom_pkg
   ```

   Assurez-vous que le basculement du package et les options de basculement des nœuds sont activés.

2. Configurez le Gestionnaire de cellule. Veillez à ne pas vous placer dans les répertoires `/etc/opt/omni` ou `/var/opt/omni` ou dans leurs sous-répertoires lorsque vous exécutez ce script. Assurez-vous également qu'il n'existe aucun sous-répertoire monté dans `/etc/opt/omni` ou `/var/opt/omni`. Exécutez :

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

3. Arrêtez les services Data Protector s'ils sont en cours d'exécution :

   ```
   /opt/omni/sbin/omnisv -stop
   ```

4. Démontez le disque partagé :

   ```
   umount disque_partagé
   ```

5. Désactivez le groupe de volumes :

   ```
   vgchange -a n nom_gv
   ```

Nœud secondaire

Connectez-vous à nouveau au nœud secondaire et procédez comme suit :

1. Redémarrez le package Data Protector :

   ```
   cmrunpkg nom_pkg
   ```

   Assurez-vous que le basculement du package et les options de basculement des nœuds sont activés.

2. Configurez le Gestionnaire de cellule. Veillez à ne pas vous placer dans les répertoires `/etc/opt/omni` ou `/var/opt/omni` ou dans leurs sous-répertoires lorsque vous exécutez ce script. Assurez-vous également qu'il n'existe aucun sous-répertoire monté dans `/etc/opt/omni` ou `/var/opt/omni`. Exécutez :

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary /share
   -upgrade
   ```

3. Arrêtez les services Data Protector s'ils sont en cours d'exécution :

   ```
   /opt/omni/sbin/omnisv -stop
   ```

4. Démontez le disque partagé :

   ```
   umount disque_partagé
   ```

5. Désactivez le groupe de volumes :

   ```
   vgchange -a n nom_gv
   ```

Nœud principal

Reconnectez-vous au nœud principal et procédez comme suit :

1. Redémarrez le package Data Protector :

   ```
   cmrunpkg nom_pkg
   ```

   Assurez-vous que le basculement du package et les options de basculement des nœuds sont activés.

2. Réimportez l'hôte virtuel :

   ```
   omnicc -import_host nom_hôte_virtuel -virtual
   ```

3. Changez le nom du Gestionnaire de cellule dans la base de données IDB :

   ```
   omnidbutil -change_cell_name
   ```

4. Si le Serveur d'installation se trouve dans le même package que le Gestionnaire de cellule, importez le nom d'hôte virtuel du serveur d'installation :

   ```
   omnicc -import_is nom_hôte_virtuel
   ```

REMARQUE :

Toutes les demandes provenant des Gestionnaires de cellule sont enregistrées dans le fichier `/var/opt/omni/log/inet.log` sur les clients. Pour empêcher l'écriture d'entrées inutiles dans le journal, sécurisez les clients. Pour plus d'informations sur la procédure de sécurisation d'une cellule, reportez-vous à la section "A propos de la sécurité" à la page 231.

Mise à niveau du Gestionnaire de cellule configuré sur Microsoft Cluster Server

La mise à niveau du Gestionnaire de cellule Data Protector A.06.00, A.06.10 ou A.06.11 vers Data Protector 6.20 sur Microsoft Cluster Server (MSCS) se fait en local, à partir du DVD-ROM d'installation Windows.

REMARQUE :

Il est recommandé d'installer MSI 2.0 sur tous les nœuds de clusters .

Conditions préalables

- L'option de mise à niveau n'est prise en charge que si le logiciel Data Protector installé auparavant est le Gestionnaire de cellule compatible cluster. Si le logiciel Data Protector est installé sur un système en tant que non compatible cluster, vous devez le désinstaller avant de procéder à l'installation.

Procédure de mise à niveau

Pour effectuer la mise à niveau, procédez comme suit :

1. Insérez le DVD-ROM d'installation Windows et exécutez la commande `\Windows_Other\i386\setup.exe`. Il est recommandé de lancer l'installation sur le noeud de serveur virtuel actuellement actif.

   Le programme d'installation détecte automatiquement l'ancienne version du produit et vous invite à la mettre à niveau vers Data Protector 6.20.

   Cliquez sur **Suivant** pour continuer.

2. Data Protector sélectionne automatiquement les composants qui ont été installés.

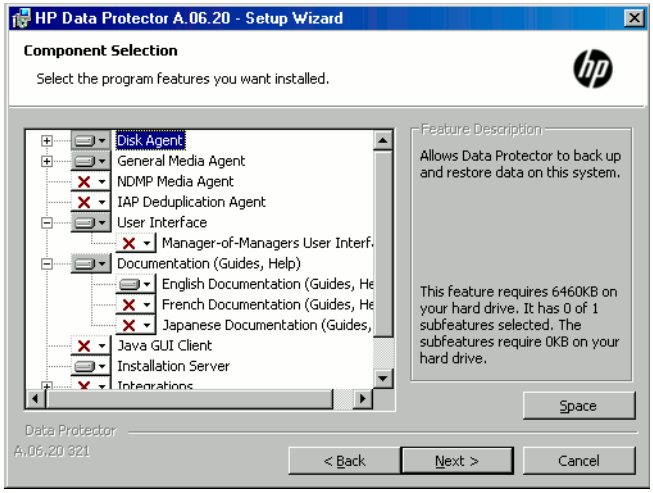


Figure 45 Sélection des composants

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.

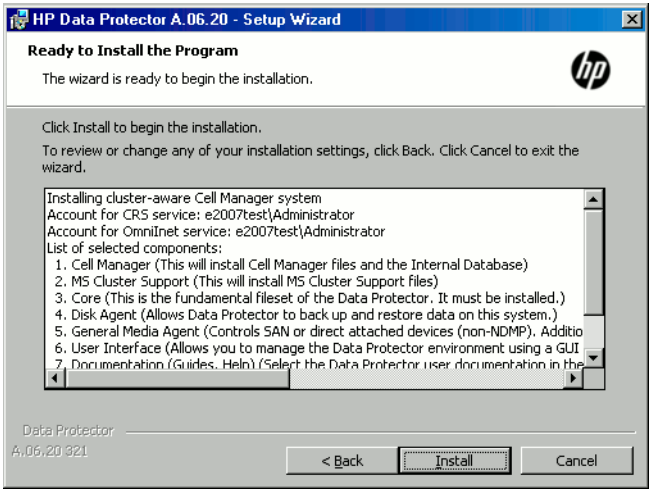


Figure 46 Page de résumé des composants sélectionnés

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

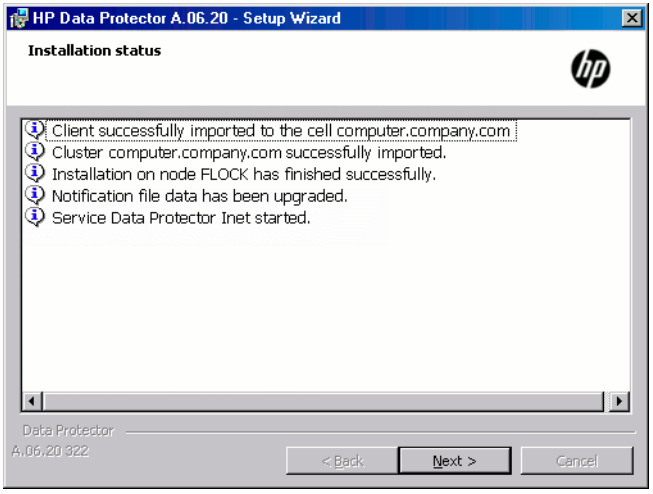


Figure 47 Page d'état de l'installation

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

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

   Il n'est *pas* recommandé d'installer l'utilitaire HP AutoPass sur Microsoft Cluster Server, car il ne serait installé que sur un seul noeud et non sur tous. Toutefois, si vous installez AutoPass, vous devez désinstaller Data Protector du même noeud sur lequel il était installé, une fois que vous décidez de supprimer Data Protector du système.

   Cliquez sur **Terminer**.

REMARQUE :

Si vous mettez à niveau des clients compatibles cluster, commencez par mettre à niveau séparément chaque nœud de cluster, puis réimportez le serveur virtuel. La mise à niveau à distance n'est pas prise en charge.

5 Attribution de licences Data Protector

Dans ce chapitre

Ce chapitre traite des sujets suivants :

- Vérification et signalement des licences Data Protector manquantes
- Obtention et installation de mots de passe permanents
- Structure de produit et licences de Data Protector

Présentation

La structure Data Protector 6.20 et de son système d'attribution de licences comprend trois catégories principales :

1. Packs Starter
2. Extensions de lecteur et extensions de bibliothèque
3. Extensions fonctionnelles

REMARQUE :

Les licences UNIX du produit fonctionnent sur toutes les plates-formes, avec le même niveau de fonctionnalité quelle que soit la plate-forme, tandis que les licences Windows fonctionnent uniquement sur les plates-formes Windows, NetWare et Linux.

Liés au Gestionnaire de cellule, les mots de passe sont valides pour l'intégralité de la cellule Data Protector. Les clients ne requièrent aucune licence pour les sauvegardes de système de fichiers ou d'image disque.

Vérification et signalement des licences

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 est stocké sur le Gestionnaire de cellule, à l'emplacement suivant : `données_programme_Data_Protector\log\server\Ob2EventLog.txt` (Windows Server 2008), `répertoire_Data_Protector\log\server\Ob2EventLog.txt` (autres systèmes Windows), ou `/var/opt/omni/server/log/Ob2EventLog.txt` (systèmes UNIX). 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, le système s'assure de la présence des licences et signale une absence éventuelle.

Les licences Data Protector sont regroupées comme suit selon leurs caractéristiques :

- Licences liées au Gestionnaire de cellule
- Licences basées sur les entités
- Licences selon 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 selon l'entité

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 SAN/toutes plates-formes et extension de lecteur pour Windows/NetWare/Linux (Intel)
- Extension pour sauvegarde en ligne d'un seul système UNIX et extension pour sauvegarde en ligne d'un seul système Windows / Linux
- Extension de cryptage Data Protector pour un système client
- Extension de restauration granulaire pour un serveur de base de données

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 selon la capacité

Les licences Data Protector basées sur la capacité sont les suivantes :

- Sauvegarde avec temps d'indisponibilité nul pour 1 To et 10 To UNIX
- Restauration instantanée pour 1 To et 10 To UNIX
- Sauvegarde avec temps d'indisponibilité nul pour 1 To et 10 To Linux
- Restauration instantanée pour 1 To et 10 To Linux
- Sauvegarde avec temps d'indisponibilité nul pour 1 To et 10 To Windows
- Restauration instantanée pour 1 To et 10 To Windows
- Sauvegarde directe via NDMP pour 1 To et 10 To
- Sauvegarde avancée sur disque pour 1 To, 10 To et 100 To

Lorsqu'une licence basée sur la capacité (autre que celle de sauvegarde avancée sur disque) est vérifiée, la quantité *totale* de l'espace disque des unités logiques sauvegardées est comparée au nombre de licences installées.

La vérification des licences est effectuée de façon à vous permettre de réaliser une restauration instantanée ou une sauvegarde même si vous avez atteint la capacité autorisée par la licence. Dans ce cas, un message d'avertissement apparaît au cours de la session de sauvegarde vous informant que vous avez dépassé la capacité autorisée par la licence.

La capacité de disque utilisée est calculée d'après les informations d'historique collectées au cours de chaque session de sauvegarde avec temps d'indisponibilité nul. 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 baie de disques ayant été utilisée 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 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 par baie de disques.

Prenons l'exemple d'un scénario avec deux baies de disques P6000 EVA. L'une des baies contient un disque unique (App.1) d'une capacité de 200 Go utilisé à des fins de 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 contient deux disques (App.2 et App.3) dont les capacités respectives sont de 150 et 120 Go. La sauvegarde est exécutée une fois par jour sur App.2 et le snapshot est supprimé une fois les données copiées sur la bande. Sur App.3, la

sauvegarde est exécutée trois fois par jour et cinq snapshots différents sont utilisés à tour de rôle à des fins de restauration instantanée. Reportez-vous à la Figure 48 à la page 331.

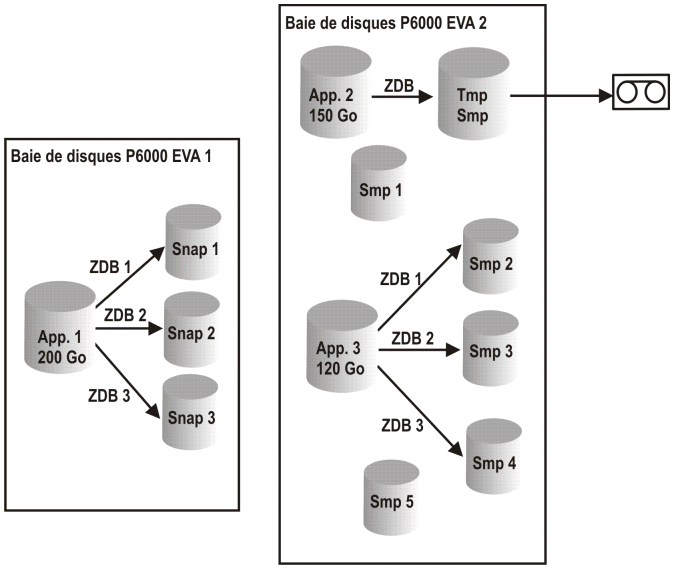


Figure 48 Scénario de calcul de la capacité utilisée

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 (App.1) + 150 Go (App.2) + 120 Go (App.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 (App.1) + 120 Go (App.3) = 320 Go.

Licence de sauvegarde avancée sur disque

La licence d'utilisation de sauvegarde avancée sur disque est nécessaire pour effectuer des sauvegardes vers une bibliothèque de fichiers Data Protector. Elle peut être utilisée pour une bibliothèque de bandes virtuelle, à la place des licences de lecteurs et de bibliothèques. Cette licence est requise par capacité native utilisable d'espace de sauvegarde sur disque en teraoctets (To).

- La capacité native utilisable d'une bibliothèque de fichiers Data Protector correspond à la taille sur disque de tous les fichiers utilisés pour la bibliothèque de fichiers, telle que l'indique le système de fichiers.
  - Les sauvegardes complètes virtuelles et les sauvegardes incrémentales à consolider en sauvegarde complète synthétique ou virtuelle doivent être stockées dans la bibliothèque de fichiers Data Protector, laquelle requiert cette licence.
- Si Data Protector utilise exclusivement la bibliothèque de bandes virtuelle, il est conseillé d'acquérir une licence pour une quantité correspondant à la capacité physique de la bibliothèque de bandes virtuelle (capacité native utilisable).
- 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 chaque bibliothèque de bandes virtuelle, vous pouvez choisir d'utiliser le modèle de licence de sauvegarde sur disque ou sur lecteur de bandes. Les deux modèles ne doivent pas être combinés dans une même bibliothèque.
  - Si la bibliothèque dispose d'une fonction intégrée pour migrer des données de sauvegarde du cache de disque vers un autre disque ou une autre bande, la capacité de stockage migrée doit faire l'objet d'une licence complète. Aucune licence de lecteur et de bibliothèque n'est requise pour la bibliothèque de bandes contrôlée exclusivement par la bibliothèque de bandes virtuelle, mais ***la capacité utilisée de toutes les bandes de la bibliothèque physique doit faire l'objet d'une licence***. Toutefois, ceci ne s'applique pas si la fonction de copie d'objet Data Protector a servi à migrer les données de sauvegarde vers un autre disque ou une autre bande.
  - Par défaut, Data Protector traite les bibliothèques de bandes virtuelles comme des bibliothèques ordinaires (comme les bibliothèques SCSI II par exemple). La licence par capacité (sauvegarde avancée sur disque) est disponible pour les bibliothèques SCSI, les contrôles externes, les bibliothèques DAS ADIC/GRAU et les bibliothèques ACS StorageTek. Pour qu'elle puisse être utilisée, le périphérique doit être identifié comme bibliothèque de bandes virtuelle pendant sa configuration. Pour plus d'informations sur la méthode de configuration d'une bibliothèque de bandes virtuelle par l'interface de ligne de commande, reportez-vous ci-après à l'Exemple à la page 333. Pour plus d'informations sur la méthode de configuration d'une bibliothèque virtuelle par l'interface utilisateur graphique, recherchez l'entrée suivante dans l'index de l'aide en ligne : "bibliothèque de bandes virtuelle".
- Dans le cas d'une gestion centrale des licences à l'aide de Manager-of-Manager (MoM), vous devez affecter au minimum 1 To à chaque cellule à l'aide de la fonction de sauvegarde avancée sur disque.

REMARQUE :

Data Protector n'est pas en mesure d'indiquer le nombre requis de licences car les bibliothèques de bandes virtuelles actuelles et certains serveurs de fichiers hébergeant la bibliothèque de fichiers ne disposent pas des interfaces et des outils adéquats. Il vous incombe d'acquérir une licence couvrant la capacité en fonction des définitions de licence.

Exemple

Si vous configurez une bibliothèque de bandes virtuelles nommée "VTL_2010" par l'intermédiaire de la commande `omniupload` lancée à partir de l'interface de ligne de commande, vous devez préciser la capacité estimée de la bibliothèque dans le fichier de configuration pour la chaîne `VTLCAPACITY`. La valeur d'estimation est ensuite ajoutée à la capacité des licences utilisées pour la sauvegarde avancée sur disque dans le rapport du vérificateur de licences.

REMARQUE :

La valeur de consommation de capacité estimée de la bibliothèque virtuelle (`VTLCAPACITY`) en téra-octets (To) doit être un nombre entier, de manière à empêcher l'apparition d'erreurs de capacité non valide.

Dans le fichier de configuration nommé "libVTL.txt" du répertoire "C:\Temp", entrez la capacité estimée de la bibliothèque, par exemple `11`, puis exécutez la commande suivante :

```
omniupload -create_library VTL_2010 -file C:\Temp\libVTL.txt
```

Pour vérifier la configuration de la bibliothèque, exécutez la commande suivante :

```
omnidownload -library VTL_2010
```

```
#omnidownload -library VTL_2010
NAME "VTL2010"
DESCRIPTION ""
HOST ordinateur.entreprise.com
POLICY SCSI-II
TYPE DDS
LIBVIRTUAL
VTLCAPACITY 11
```

```
IOCTLSERIAL ""
CONTROL "Adresse SCSI"
REPOSITORY "Référentiel SCSI"
MGMTCONSOLEURL ""
```

Le vérificateur de licence renvoie la capacité de licence utilisée, à savoir la somme de l'espace disque utilisé pour la bibliothèque de fichiers et la taille estimée de l'espace disque d'une bibliothèque de bandes virtuelle. Par exemple, vous utilisez 2 To de l'espace disque en effectuant des sauvegardes avec la bibliothèque de fichiers et 10 To de capacité dans la bibliothèque de bandes virtuelle. La capacité totale utilisée est de 12 To. S'il la capacité de licence installée n'est que de 5 To, un message de notification vous informe que vous avez besoin de 7 licences de sauvegarde avancée sur disque pour 1 To supplémentaires.

```
#omnicc –check_licenses –detail
------------------------------------------------------------------
License Category               : Advanced Backup to disk for 1 TB
Licenses Capacity Installed    : 5 TB
Licenses Capacity In Use       : 12.0 TB
Add. Licenses Capacity Required: 7 TB

Summary
-------
Description                                      Licenses Needed
Advanced Backup to disk for 1 TB                               7
```

Exemples de licences basées sur la capacité

Ce paragraphe fournit des exemples illustrant la manière dont les licences basées sur la capacité sont attribuées.

Exemple 1

La Figure 49 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 ZDB sur disque.

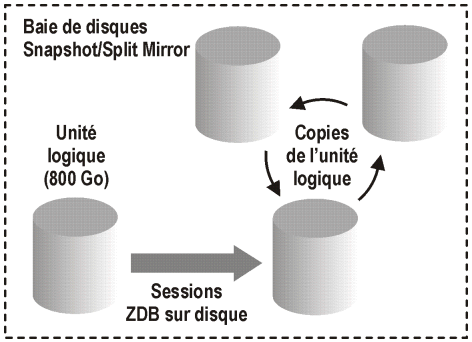


Figure 49 Sessions de sauvegarde avec temps d'indisponibilité nul sur disque

Trois copies Split Mirror ou Snapshot (répliques) font l'objet d'une rotation et conservées à des fins de restauration instantanée. L'attribution de la licence basée sur la capacité est calculée de la manière suivant :

Une unité logique de 800 Go est utilisée pour les sessions ZDB sur disque :

1 x 800 Go = 0,8 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

Trois répliques 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 dans ce cas.

Exemple 2

La Figure 50 à la page 336 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.

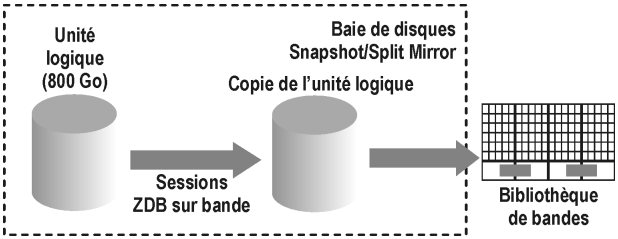


Figure 50 Sessions de sauvegarde avec temps d'indisponibilité nul sur bande

Exemple 3

La Figure 51 à la page 337 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.

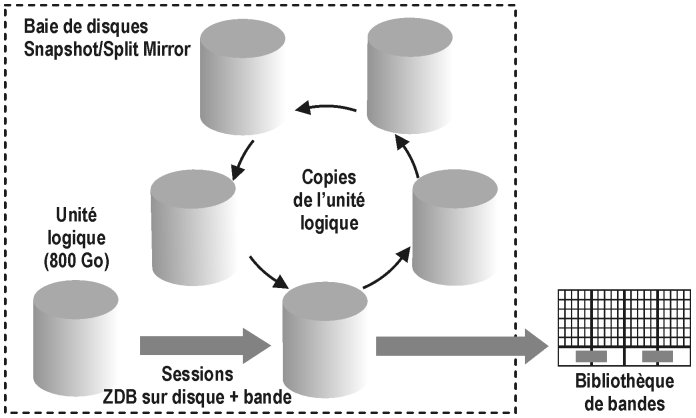


Figure 51 Sessions avec temps d'indisponibilité nul sur disque + bande

Exemple 4

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'une unité logique de 200 Go, d'une unité logique de 120 Go et d'une unité logique de 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 licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To" et une licence "Restauration instantanée pour 1 To" sont suffisantes si les trois exemples des illustrations Figure 49 à la page 335 à Figure 51 à la page 337 sont configurés dans une cellule.

Production d'un rapport de licences sur demande

Pour générer un rapport sur les licences de la cellule, exécutez :

```
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. Les informations suivantes sont renvoyées : heure de création du rapport, mode d'attribution de licences et serveur de licences.

Si l'option `-detail` est spécifiée, un rapport détaillé est généré. Le vérificateur de licences renvoie les informations suivantes pour chaque licence de la cellule : nom de la licence, licences installées, licences utilisées et licences supplémentaires (capacité) requises.

Notez que, pour les licences d'utilisation de l'extension de lecteur, le vérificateur de licences renvoie des informations sur les lecteurs configurés et les licences supplémentaires recommandées. 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.

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 connaître les dates d'expiration des licences, exécutez :

```
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.

Pour plus d'informations, reportez-vous à la page de manuel `omnicc` ou au document *Guide de référence de l'interface de ligne de commande HP Data Protector*.

Vérification et identification des licences pré-Data Protector 6.20

Dans Data Protector 6.20 le vérificateur de licences mappe certaines licences de versions précédentes sur la nouvelle structure de produit Data Protector 6.20 et les identifie comme de nouvelles licences. Notez que certaines limitations peuvent toujours survenir au cours de la mise en application des licences. Pour plus d'informations, consultez les limitations dans les *Références, notes de publication et annonces produits HP Data Protector*.

Ce chapitre traite des sujets suivants :

- "Signalement des anciennes licences de sauvegarde avec temps d'indisponibilité nul et de restauration instantanée" à la page 344

Identification des licences de serveurs de lecteurs multiples

La licence d'utilisation de serveur de lecteurs multiples pour UNIX est identifiée en tant que 6 licences d'extension de lecteur pour SAN / toutes plates-formes.

Notez que la licence de lecteurs multiples s'utilise uniquement sur un serveur de périphériques si l'option **Le client est serveur de périphériques** est définie dans le contexte **Client** de l'onglet **Avancé** lorsque vous sélectionnez un client dans l'interface graphique. Si cette option n'est pas configurée, la licence de lecteurs multiples n'est pas utilisée, même si elle est installée.

Le nombre de licences d'extension de lecteur pour SAN / toutes plates-formes installées est augmenté de 6. Par exemple, vous disposez d'une (1) licence de serveur de lecteurs multiples pour UNIX et d'une (1) licence d'extension de lecteur pour SAN / toutes plates-formes, installées sur un serveur de périphériques. Le vérificateur de licences indique que 7 licences d'extension de lecteur pour SAN / toutes plates-formes sont installées (1 lecteur simple + 6 pour 1 lecteur multiple).

Si 10 lecteurs sont configurés dans un système, le vérificateur de licence signale que 3 licences d'extension de lecteur pour SAN / toutes plates-forme sont recommandées pour permettre l'utilisation simultanée de tous les lecteurs.

```
#omnicc –check_licenses –detail
License Category         : Drive extension for SAN / all platforms
Licenses Installed       : 7
Drives Configured        : 10
Add. Licenses Recommended: 3

Summary Description              Add. Drive Licenses Recommended
Drive extension for SAN / all platforms                         3

WARNING: At any given moment, you need as many licenses as there
are drives in use for any operation, such as formatting, backup,
restore, media and object copying, media and object verifying,
object mirroring, scanning, and disaster recovery. To allow all
drives to be used simultaneously, you need as many licenses as
there are configured drives.

Licensing is covered.
```

Licences des systèmes Windows subissent un traitement identique. La licence de serveur de lecteurs multiples pour Windows / NetWare est supprimée du rapport

du vérificateur de licences et elle est identifiée comme 4 licences d'extension de lecteur pour Windows / NetWare / Linux. Le nombre de licences d'extension de lecteur pour Windows / NetWare / Linux augmente de 4. Dans un environnement comprenant 10 lecteurs configurés et dans lequel une (1) licence de lecteurs multiples et une (1) licence de lecteur simple sont installées, le vérificateur signale que 5 licences d'extension de lecteur (10 requises, 5 couvertes : 4 d'un lecteur multiple, 1 d'un lecteur simple) sont recommandées pour permettre l'utilisation simultanée des lecteurs.

```
#omnicc –check_licenses –detail
License Category: Drive extension for Windows / NetWare / Linux
Licenses Installed       : 5
Drives Configured        : 10
Add. Licenses Recommended: 5

Summary
Description                     Add. Drive Licenses Recommended
Drive extension for SAN / all platforms                      5

WARNING: At any given moment, you need as many licenses as there
are drives in use for any operation, such as formatting, backup,
restore, media and object copying, media and object verifying,
object mirroring, scanning, and disaster recovery. To allow all
drives to be used simultaneously, you need as many licenses as
there are configured drives.

Licensing is covered.
```

Il existe également d'anciennes licences combinées, à savoir du Gestionnaire de cellule et serveur de lecteurs multiples pour UNIX et du Gestionnaire de cellule et serveur de lecteurs multiples pour Windows / NetWare.

Si une (1) licence Gestionnaire de cellule et serveur de lecteurs multiples pour UNIX est installée, la commande `omnicc` signale qu'une (1) licence de Gestionnaire de cellule pour toutes les plates-formes et une (1) licence de serveur de lecteurs multiples pour UNIX sont installées.

```
#omnicc
Licensing mode     : Local
License server     : ordinateur.entreprise.com

Category                       Number of Licenses
Cell Manager for all platforms                   1
Cell Manager for Windows / Linux                 0
Drive extension for SAN / all platforms          0
```

```
Drive extension for Windows / NetWare / Linux                  0
Multi-Drive Server for UNIX                                    1
Multi-Drive Server for Window / NetWare                        0
```

Cette licence d'utilisation combinée est identifiée comme une (1) licence Gestionnaire de cellule et serveur de lecteur unique pour UNIX et 5 licences d'extension de lecteur pour SAN / toutes plates-formes. Cela signifie que le vérificateur de licences signale 1 licence de Gestionnaire de cellule pour toutes les plates-formes et 6 licences d'extension de lecteur pour SAN / toutes plates-formes.

Si 10 lecteurs sont configurés dans votre système et une (1) licence Gestionnaire de cellule et serveur de lecteurs multiples est installée, le vérificateur signale que 4 licences d'extension de lecteur pour SAN / toutes plates-formes (10 requises, 6 couvertes) sont recommandées.

```
#omnicc –check_licenses –detail
License Category           : Cell Manager for all platforms
Licenses Installed         : 1
Licenses Used              : 1
Additional Licenses Required: 0

License Category: Drive extension for Windows / NetWare / Linux
Licenses Installed         : 6
Drives Configured          : 10
Add. Licenses Recommended  : 4

Summary Description                   Add. Drive Licenses Recommended
Drive extension for SAN / all platforms                      4

WARNING: At any given moment, you need as many licenses as there
are drives in use for any operation, such as formatting, backup,
restore, media and object copying, media and object verifying,
object mirroring, scanning, and disaster recovery. To allow all
drives to be used simultaneously, you need as many licenses as
there are configured drives.

Licensing is covered.
```

L'ancienne licence combinée pour les systèmes Windows subit un traitement identique. La licence Gestionnaire de cellule et serveur de lecteurs multiples pour Windows / NetWare est identifiée comme une (1) licence Gestionnaire de cellule et serveur de lecteur unique pour Windows et 4 licences d'extension de lecteur pour Windows / NetWare / Linux. Le vérificateur de licences signale qu'une (1) licence Gestionnaire de cellule pour Windows / Linux et 5 licences d'extension de lecteur pour Windows / NetWare / Linux sont installées.

Bien que le vérificateur de licences soit désormais en mesure de signaler les licences manquantes, la vérification des licences au cours de la sauvegarde n'est pas modifiée. Lorsque la licence de lecteurs multiples est installée sur un serveur de lecteurs, il est toujours possible d'utiliser simultanément un nombre illimité de lecteurs configurés. En revanche, si aucun serveur de lecteurs n'est configuré, mais que la licence de lecteurs multiples est installée, la sauvegarde peut s'avérer impossible, même si le vérificateur de licences signale qu'un nombre suffisant de licences de lecteur unique sont installées.

Identification des anciennes licences de sauvegarde en ligne

Les licences d'utilisation de l'extension de sauvegarde en ligne pour le système UNIX et de l'extension de sauvegarde en ligne pour les systèmes Windows / Linux sont valides pour tous les clients d'une cellule. Les licences de sauvegarde en ligne de précédentes versions de Data Protector augmentent de 1 le nombre de licences en vigueur installées.

Le vérificateur de licences peut désormais signaler que des licences de sauvegarde en ligne supplémentaires sont requises s'il existe un grand nombre de systèmes dans une cellule. Par exemple, il y a 5 systèmes Windows utilisant la sauvegarde en ligne dans une cellule et une (1) licence d'extension de sauvegarde en ligne pour Windows. Comme 1 système est couvert par la licence installée, 4 autres sont requis pour les 4 autres systèmes. Le vérificateur de licence signale que 4 licences d'extension de sauvegarde en ligne pour UN SEUL système Windows / Linux sont requises.

```
#omnicc –check_licenses –detail
License Category: On–line Extension for ONE Windows / Linux system
Licenses Installed    : 1
Licenses Used         : 5
Add. Licenses Required: 4

Summary Description                                Licenses Needed
On-line Extension for ONE Windows / Linux system                4

Licensing is NOT covered.
```

Si 3 licences d'extension de sauvegarde en ligne pour UN SEUL système Windows / Linux sont installées, vous êtes informé qu'une (1) licence d'extension de sauvegarde en ligne pour UN SEUL système Windows / Linux (5 requises, 4 couvertes : 1 pour l'ancienne et 3 pour UN SEUL système) est toujours requise :

```
#omnicc –check_licenses –detail
License Category: On-line Extension for ONE Windows / Linux system
```

```
Licenses Installed    : 4
Licenses Used         : 5
Add. Licenses Required: 1

Summary
Description                                          Licenses Needed
On-line Extension for ONE Windows / Linux system                   1

Licensing is NOT covered.
```

Identification des licences pour la sauvegarde directe par NDMP

La licence d'utilisation de l'extension pour UN SEUL serveur NDMP est identifiée comme 1 licence de sauvegarde directe via NDMP pour 1 To. La première est une licence basée sur entité, à savoir qu'une (1) licence est nécessaire pour 1 serveur NDMP. La licence de sauvegarde directe via NDMP pour 1 To, est une licence fondée sur la capacité, à savoir qu'elle est requise pour sauvegarder 1 To sur 1 serveur NDMP.

La capacité en quantité de licences installées pour la licence de sauvegarde directe via NDMP pour 1 To augmente du nombre de licences d'extension pour UN SEUL serveur NDMP installées. Par exemple, 1 licence de sauvegarde directe via NDMP pour 1 To te 1 licence de sauvegarde directe via NDMP pour 1 To installées donnent conjointement une capacité de licences installées de 2 To. En conséquence, le vérificateur de licences peut maintenant signaler que des licences supplémentaires sont requises. Par exemple, vous sauvegardez jusqu'à 5 To via NDMP et vous avez installé une (1) licence d'extension pour UN SEUL serveur NDMP et 1 licence de sauvegarde directe vida NDMP pour 1 To. Le vérificateur de licences signale que 3 licences de sauvegarde directe via NDMP pour 1 To sont requises (5 nécessaires, 2 couvertes : 1 de l'ancienne et 1 de la nouvelle licence).

```
#omnicc –check_licenses –detail
License Category               : Direct Backup using NDMP for 1 TB
Licenses Capacity Installed    : 2 TB
Licenses Capacity In Use       : 5.0 TB
Add. Licenses Capacity Required: 3 TB

Summary
Description                                        Licenses Needed
Direct Backup using NDMP for 1 TB                                3
```

Identification des licences de bibliothèques d'emplacements

Les licences d'utilisation des extensions spécifiques aux plates-formes, à savoir 1 pour Windows et 1 pour les systèmes UNIX, sont signalées comme licences indépendantes des plates-formes.

Le nombre de licences Extension pour UNE SEULE bibliothèque de 61 à 250 emplacements installées est augmenté du nombre de licences spécifiques à la plate-forme installée pour des bibliothèques de 61 à 250 emplacements et les licences illimitées spécifiques à la plate-forme sont ajoutées au nombre de licences Extension pour UNE SEULE bibliothèque sans limitations en nombre d'emplacement installées.

Si vous avez installé une (1) licence Extension pour bibliothèque sans limitations en nombre d'emplacements pour UNIX et une (1) licence Extension pour bibliothèque sans limitations en nombre d'emplacements pour Windows, le vérificateur de licences signale que 2 licences Extension pour UNE SEULE bibliothèque sans limitations en nombre d'emplacements sont installées.

```
#omnicc –check_licenses –detail
License Category      : Extension for ONE 61-250 Slot Library
Licenses Installed    : 2
Licenses Used         : 0
Add. Licenses Required: 0
License Category      : Extension for ONE Unlimited Slot Library
Licenses Installed    : 2
Licenses Used         : 0
Add. Licenses Required: 0
```

En raison des licences ne dépendant pas de la plate-forme des bibliothèques d'emplacements, la mise en application des licences est plus puissante que leur vérification. Au cours de la sauvegarde, Data Protector vérifie les licences de différentes plates-formes et la sauvegarde peut s'avérer impossible du fait de l'absence de licences pour une plate-forme spécifique, même si le vérificateur signale qu'un nombre suffisant de licences appropriées est installé sur le système.

Signalement des anciennes licences de sauvegarde avec temps d'indisponibilité nul et de restauration instantanée

- La licence d'utilisation de sauvegarde avec temps d'indisponibilité nul pour 1 To (B7025CA) remplace les licences de sauvegarde avec temps d'indisponibilité nul spécifiques à la baie de disques des versions précédentes de Data Protector :
  - Sauvegarde avec temps d'indisponibilité nul pour 1 To pour HP StorageWorks Modular SAN Array 1000 (`Sauvegarde avec temps`

`d'indisponibilité nul pour 1 To pour HP StorageWorks Modular SAN Array 1000` (B7036AA))

- Sauvegarde avec temps d'indisponibilité nul pour 1 To pour HP StorageWorks P6000 EVA Disk Array Family (`Sauvegarde avec temps d'indisponibilité nul pour 1 To (licence générique)` (B7025CA))
- Sauvegarde avec temps d'indisponibilité nul pour 1 To pour HP StorageWorks P9000 XP Disk Array Family (`Sauvegarde avec temps d'indisponibilité nul pour 1 To pour HP StorageWorks XP` (B7023CA))
- Sauvegarde avec temps d'indisponibilité nul pour 1 To pour EMC Symmetrix / DMX (`Sauvegarde avec temps d'indisponibilité nul pour 1 To pour EMC Symmetrix / DMX` (B6959CA))

Toutes les licences spécifiques d'une baie de disques sont identifiées par le vérificateur de licences comme 1 licence générique de sauvegarde avec temps d'indisponibilité nul pour 1 To (B7025CA). La quantité de licences génériques installées est augmentée du nombre de toutes les licences spécifiques au type de baie de disques. La capacité de licence utilisée est la somme des données utilisées sur toutes les baies. Par exemple, vous avez installé 1 licence pour chaque catégorie de license spécifique d'une baie de disques, conjointement avec 4 licences de sauvegarde avec temps d'indisponibilité nul. Vous sauvegardez 2 To sur EMC Symmetrix, 2 To sur P9000 XP Array et 6 To sur P6000 EVA Array. En conséquence, vous avez besoin de 10 mais n'en disposez que de 4. Le vérificateur de licence signale que 6 licences de sauvegarde avec temps d'indisponibilité nul pour 1 To supplémentaires sont requises (10 nécessaires, 4 installées).

```
#omnicc –check_licenses -detail
------------------------------------------------------------
License Category               : Zero Downtime Backup for 1 TB
Licenses Capacity Installed    : 4 TB
Licenses Capacity In Use       : 10.0 TB
Add. Licenses Capacity Required: 6 TB

Summary
-------
Description                                  Licenses Needed
Zero Downtime Backup for 1 TB                              6

Licensing is NOT covered.
```

Notez que les anciennes licences de sauvegarde avec temps d'indisponibilité nul sans limitations pour EMC Symmetrix et P9000 XP Array sont identifiées comme suit :

- Licences Extension pour EMC Split Mirror (B6959AA) en tant que 3 licences de sauvegarde avec temps d'indisponibilité nul pour EMC Symmetrix / DMX 1 To (B6959CA)
- Licences Extension pour HP XP Split Mirror (B7023AA) en tant que 3 licences de sauvegarde avec temps d'indisponibilité nul pour HP StorageWorks XP 1 To (B7023CA)
- Licences Extension de sauvegarde avec temps d'indisponibilité nul pour UN SEUL EMC Symmetrix (B6959BA) en tant que 3 licences de sauvegarde avec temps d'indisponibilité nul pour EMC Symmetrix / DMX 1 To (B6959CA)
- Licences Extension de sauvegarde avec temps d'indisponibilité nul pour UN SEUL système HP StorageWorks XP (B7023BA) en tant que 3 licences de sauvegarde avec temps d'indisponibilité nul pour HP StorageWorks XP 1 To (B7023CA)

Autrement dit, les anciennes licences pour EMC Symmetrix et P9000 XP Array sont également identifiées comme 3 licences de sauvegarde avec temps d'indisponibilité nul pour 1 To.

Par exemple, si vous avez installé sur votre système 1 licence de sauvegarde avec temps d'indisponibilité nul pour chaque catégorie de licence, le vérificateur signale 16 licences d'utilisation de sauvegarde avec temps d'indisponibilité nul pour 1 To installées (1+1+1+1+3+3+3+3).

- La licence d'utilisation de restauration instantanée pour 1 To (B7028AA) remplace les licences restauration instantanée spécifiques à la baie de disques des versions précédentes de Data Protector :
  - Restauration instantanée pour 1 To pour HP StorageWorks Modular SAN Array 1000 (`Restauration instantanée pour 1 To pour HP StorageWorks Modular SAN Array 1000` (B7037AA))
  - Restauration instantanée pour 1 To pour HP StorageWorks P6000 EVA Disk Array Family (`Restauration instantanée pour 1 To (licence générique)` (B7028AA))
  - Restauration instantanée pour 1 To pour HP StorageWorks P9000 XP Disk Array Family (`Restauration instantanée pour 1 To pour HP StorageWorks XP` (B7026CA))

  Toutes les licences spécifiques d'une baie de disques sont identifiées par le vérificateur de licences comme 1 licence générique de restauration instantanée pour 1 To. La quantité de licences génériques installées est augmentée du nombre de toutes les licences spécifiques d'une baie de disques. La capacité de licence est la somme des données utilisées sur toutes les baies.

```
#omnicc –check_licenses -detail
------------------------------------------------------
License Category               : Instant Recovery for 1 TB
Licenses Capacity Installed    : 3 TB
Licenses Capacity In Use       : 5.0 TB
Add. Licenses Capacity Required: 2 TB

Summary
-------
Description                                  Licenses Needed
Instant Recovery for 1 TB                                  2

Licensing is NOT covered.
```

Notez que la mise en application des licences est plus puissante que la vérification des licences. Au cours de la sauvegarde avec temps d'indisponibilité nul, la sauvegarde peut s'avérer impossible en raison de l'absence des licences associées à une baie de stockage spécifique, même si le vérificateur de licences signale un nombre suffisant de licences de sauvegarde avec temps d'indisponibilité nul et de restauration instantanée.

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 permanent vous permet de configurer une cellule Data Protector en fonction de votre stratégie de

sauvegarde, à condition d'avoir 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 AutoPass, qui peut être installé pendant le processus d'installation du Gestionnaire de cellule. Pour connaître les instructions sur l'obtention de mots de passe avec l'utilitaire HP AutoPass une fois ce dernier installé pendant le processus d'installation du Gestionnaire de cellule, reportez-vous à la section "Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass" à la page 348.

Reportez-vous à la section "Autres moyens d'obtenir et d'installer des mots de passe permanents" à la page 351 pour connaître les instructions sur l'obtention et l'installation d'un mot de passe par un autre moyen que l'utilitaire HP AutoPass.

Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass

L'utilitaire HP AutoPass permet d'installer directement via Internet des mots de passe pour les licences achetées pour vos produits HP, à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus d'informations sur l'utilitaire HP AutoPass, reportez-vous à l'aide en ligne de l'utilitaire HP.

Configuration système requise

Pour obtenir et installer des mots de passe permanents à l'aide de l'utilitaire HP AutoPass, assurez-vous que les conditions suivantes sont remplies :

- Installez l'utilitaire HP AutoPass avec le Gestionnaire de cellule. Si vous n'avez pas installé cet utilitaire sur votre système avant d'installer Data Protector, vous pouvez le faire à l'aide du script `omnisetup.sh` (systèmes UNIX) ou pendant l'installation du Gestionnaire de cellule (systèmes Windows).
- Installez Java Runtime Environment (JRE) 1.5.0_06 ou toute version supérieure sur le Gestionnaire de cellule.
- Sur MC/ServiceGuard, l'utilitaire HP AutoPass doit être installé sur tous les 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.
- Avant d'installer AutoPass sur HP-UX 11.23 (Itanium), vérifiez que les correctifs suivants sont installés :
  - PHSS_36343 1.0 aC++ Runtime (IA : A.06.15, PA : A.0376)
  - PHSS_37039 1.0 Integrity Unwind Library

Limites

Les limites suivantes s'appliquent à l'utilitaire HP AutoPass :

- L'utilitaire HP AutoPass n'est pas installé sur les systèmes d'exploitation Windows 2003 x64, Windows Vista x64, Windows Server 2008 x64 et Linux.
- Il n'est *pas* recommandé d'installer HP AutoPass sur Microsoft Cluster, car il ne serait installé que sur un seul nœud et non sur tous.
- La commande `omniinstlic` ne fonctionne que si JRE 1.5.0_06 (ou une version supérieure) est installé sur le Gestionnaire de cellule.

Pour plus d'informations sur les conditions requises et les limitations, reportez-vous à l'aide en ligne de l'utilitaire HP AutoPass.

Les mots de passe sont installés sur le Gestionnaire de cellule et sont valides pour l'intégralité de la cellule.

Procédure

Pour obtenir et installer un mot de passe permanent, procédez comme suit :

1. Rassemblez les informations nécessaires à l'obtention d'un mot de passe permanent. Consultez l'aide en ligne de l'utilitaire HP AutoPass pour connaître les informations requises.

2. Commandez le mot de passe en ligne à l'aide de l'utilitaire *HP AutoPass*. Pour lancer l'*utilitaire HP AutoPass*, exécutez la commande suivante sur le Gestionnaire de cellule :

REMARQUE :

Dans un environnement Manager-of-Managers (MoM), la commande `omniinstlic` doit être exécutée soit sur le système MoM (si vous *utilisez* une attribution centralisée des licences Data Protector), soit sur le Gestionnaire de cellule auquel les mots de passe commandés et installés sont destinés (si vous *n'utilisez pas* l'attribution centralisée des licences Data Protector).

`/opt/omni/sbin/omniinstlic` (Gestionnaire de cellule UNIX) ou

`répertoire_Data_Protector``\bin\omniinstlic` (Gestionnaire de cellule Windows)

Pour plus d'informations, reportez-vous à la page `omniinstlic` du manuel ou au *Guide de référence de l'interface de ligne de commande HP Data Protector*.

3. Suivez les instructions de l'assistant de l'*utilitaire HP AutoPass* et entrez les informations requises.

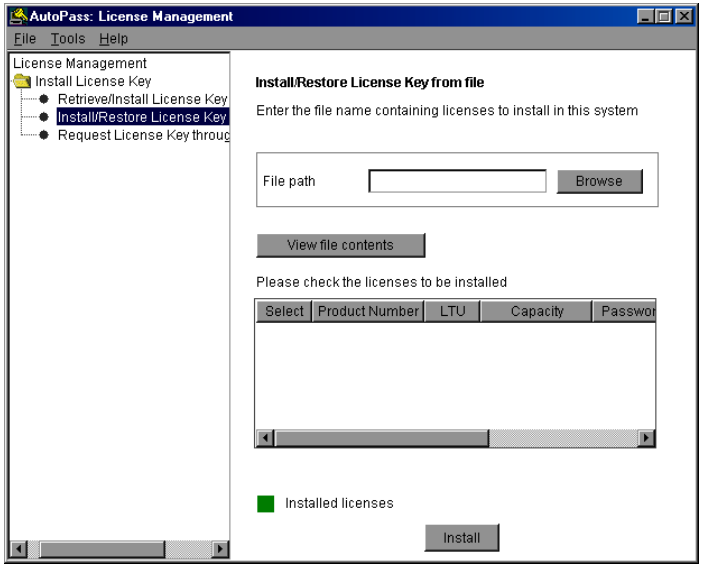


Figure 52 Assistant de l'utilitaire HP AutoPass

A la dernière étape de l'assistant, cliquez sur **Obtenir mot de passe** pour transférer les mots de passe permanents des licences achetées du *Centre de remise de mot de passe HP* vers le Gestionnaire de cellule.

Cliquez sur **Terminer** pour installer les mots de passe permanents des licences achetées sur le Gestionnaire de cellule.

4. Pour obtenir des instructions de vérification des mots de passe installés, reportez-vous à la section "Vérification du mot de passe" à la page 355.

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 362 pour trouver l'emplacement des formulaires et obtenir des instructions pour les remplir.

2. Pour plus d'informations sur la structure des produits, reportez-vous à la section "Structure de produit et licences de Data Protector 6.20" à la page 358. 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 :
       - Avec le Gestionnaire de cellule Windows : `répertoire_Data_Protector\Docs\license_forms.txt`
       - Avec le Gestionnaire de cellule UNIX : `/opt/omni/doc/C/license_forms_UNIX`
       - Sur le DVD-ROM d'installation Windows : `Nom_disque:\Docs\license_forms.txt`

       pour "copier" et "coller" votre message au *Centre de remise de mot de passe HP (HP PDC)*.

       Votre mot de passe permanent vous sera envoyé dans les 24 heures suivant l'envoi du *Formulaire de demande de mot de passe permanent*.

Installation

Cette section indique la procédure à suivre pour installer un mot de passe permanent transmis par le *Centre de remise de mot de passe HP (HP PDC)* :

Condition préalable

Le *Centre de remise de mot de passe HP* doit vous avoir envoyé les mots de passe permanents et l'interface utilisateur de 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 utilisateur graphique

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. Indiquez le mot de passe exactement tel qu'il figure sur le *certificat de mot de passe*.

   Un mot de passe se compose de 8 groupes de 4 caractères chacun, séparés par un espace et suivis par une chaîne. Assurez-vous que cette séquence ne contient ni saut de ligne, ni retour chariot. Vous trouverez ci-après un exemple de mot de passe :

   ```
   2VFF 9WZ2 C34W 43L7 RYY7 HBYZ S9MQ 1LZA JUUQ TA48 EPNB
   QFRN MR9F 2A2A 7UEG 9QR3 Y3QW LZA9 AZA9 EQ97 "Produit;
   Gestionnaire de cellule UNIX"
   ```

   Après avoir saisi le mot de passe, effectuez les vérifications suivantes :

   - Assurez-vous que le mot de passe s'affiche correctement à l'écran.
   - Vérifiez qu'il n'y a pas d'espace en tête ou à la fin du mot de passe, ni de caractères en trop.
   - Vérifiez que vous n'avez pas confondu les caractères "1" (le chiffre) et "l" (la lettre).
   - Vérifiez que vous n'avez pas confondu les caractères "O" (lettre majuscule) et "0" (chiffre).
   - Vérifiez que vous avez utilisé la bonne casse. Le mot de passe tient compte de la casse.

   Cliquez sur **OK**.

Le mot de passe est enregistré dans le fichier suivant sur le Gestionnaire de cellule :

- Sous Windows Server 2008 : `données_programme_Data_Protector\Config\server\Cell\lic.dat`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\Config\server\Cell\lic.dat`
- Sur les systèmes UNIX : `/etc/opt/omni/server/cell/lic.dat`

Utilisation de l'interface de ligne de commande

Pour installer le mot de passe permanent via l'interface de ligne de commande (CLI) de Data Protector, procédez comme suit :

1. Connectez-vous au Gestionnaire de cellule.
2. Exécutez la commande suivante :
   - Sous Windows :

     ```
     répertoire_Data_Protector\bin\omnicc -install_license mot de passe
     ```

   - Sous UNIX : `/opt/omni/bin/omnicc -install_license mot de passe`

   Le `mot de passe` doit être saisi tel qu'il apparaît dans le *Certificat de mot de passe*. Il doit figurer sur une seule ligne et ne contenir aucun caractère de retour chariot. Le mot de passe doit être placé entre apostrophes. Si le mot de passe comporte également une description entre apostrophes, ces dernières doivent être précédées d'une barre oblique inverse. Pour obtenir un exemple et plus d'informations, reportez-vous à la page de manuel `omnicc` ou au *Guide de référence de l'interface de ligne de commande HP Data Protector*.

Vous pouvez également ajouter le mot de passe dans le fichier suivant sur le Gestionnaire de cellule :

- Sous Windows Server 2008 : `données_programme_Data_Protector\config\server\cell\lic.dat`
- Sur les autres systèmes Windows : `répertoire_Data_Protector\config\server\cell\lic.dat`
- Sur les systèmes UNIX : `/etc/opt/omni/server/cell/lic.dat`

Si ce fichier n'existe pas, créez-en un avec un éditeur tel que `vi` ou `Bloc-notes`. Pour obtenir un exemple de mot de passe, reportez-vous à l'Étape 3 à la page 353 de la procédure faisant appel à l'interface utilisateur graphique.

Vérification du mot de passe

Utilisation de l'interface utilisateur graphique

Pour vérifier que le mot de passe pour la licence que vous avez installée est correct, procédez comme suit dans l'interface utilisateur graphique de Data Protector :

1. Dans le menu Aide, cliquez sur **A propos de**.
2. Cliquez sur l'onglet **Licence**. Toutes les licences installées s'affichent. Si le mot de passe que vous avez saisi n'est pas correct, il est accompagné de la remarque `Impossible de décoder le mot de passe.`

Utilisation de l'interface de ligne de commande

Pour vérifier que le mot de passe pour la licence que vous avez installée est correct, utilisez la commande suivante :

- Sous Windows :

  `répertoire_Data_Protector\bin\omnicc -password_info`
- Sous UNIX : `/opt/omni/bin/omnicc -password_info`

Cette commande affiche toutes les licences installées. Si le mot de passe que vous avez saisi n'est pas correct, il est accompagné de la remarque `Impossible de décoder le mot de passe.`

Recherche du nombre de licences installées

Utilisation de l'interface utilisateur graphique

Après avoir installé un mot de passe permanent, vous pouvez vérifier le nombre de licences actuellement installées sur le Gestionnaire de cellule :

1. Lancez 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 362.

   Dans le formulaire, vous devez spécifier le nombre de licences à déplacer du Gestionnaire de cellule existant.
2. Supprimez le fichier suivant :
   - Sous Windows Server 2008 : `données_programme_Data_Protector\config\server\cell\lic.dat`
   - Sur les autres systèmes Windows : `répertoire_Data_Protector\config\server\cell\lic.dat`
   - Sur les systèmes UNIX : `/etc/opt/omni/server/cell/lic.dat`

3. Après avoir rempli le *formulaire de déplacement de licence* et l'avoir envoyé 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".

Structure de produit et licences de Data Protector 6.20

Cette section décrit l'utilisation de la structure de produit Data Protector afin de faciliter l'identification des numéros de produit à commander.

La structure de produit se divise en plusieurs sections, comme indiqué dans la Figure 53 à la page 359. Lorsque vous commandez une solution Data Protector, procédez comme suit :

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 fonctionnalités recommandées peuvent aller de la sauvegarde en ligne à la 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.

Guide d'une page sur la structure de produit DP 6.2 pour les licences

	Edition serveur unique	Ttes plates-formes	Windows	HP-UX		Solaris
	Licence seulement / migration vers Pack Starter DVD seulement (langue à sélectionner)	Par langue*	B7030BA/B7031AA	B7020BA/B7021AA		B7020CA/B7021DA
1	**Packs Starter** (requis)	Ttes plates-formes	Windows	Linux	HP-UX	Solaris
1	Licence seulement DVD seulement 1x cellule (langue à sélectionner)	Par langue*	B6961BA	B6961CA	B6951BA	B6951CA
	Extensions lecteurs et bibliothèques	Ttes plates-formes	Windows, NetWare, Linux		SAN, UNIX, NAS	
	Licence lecteur Licence bibliothèque 1x lecteur 1x 61-250/empl. illimités 1x mise à niveau empl. illim	B6957BA/B6958BA B6958CA	B6963AA		B6953AA	
2	**2. Manager of Managers**		Windows et Linux		UNIX	
2	Licence MOM 1x système		B6966AA		B6956AA	
3	**3. Sauvegarde sur disque**	Ttes plates-formes				
3	Lic. sauv. avanc. disque 1xTo/10xTo/100xTo	B7038AA/BA/CA				
4	**4. Protection des applications**	Ttes plates-formes	Windows	Linux	UNIX	
4	Licence sauv. en ligne 1x système		B6965BA		B6955BA	
4	Licence ZDB 1x To /10x To Licence rest. instantanée 1x To /10x To		Réf. Spéc. rapides* Réf. Spéc. rapides*	B7025CA/B7025DA B7028AA/B7028DA		
	Ext. restauration granul. 1x système	TB737AA				
	Licence ext. portable 1x 100 / 1 000 clients	TA032AA/TA033AA			CD slmt	TA031AA
	Lic. sauv. fichiers ouverts 1x serveur entp./5x postes 1x 1 serveur/1x10 serveurs	BA155AA/BA154AA BA153AA/BA153BA			CD slmt	BA152AA
	Licence cryptage 1x 1 serveur/1x10 serveurs	BB618AA/BB618BA				
	Licence Media Operations 1x2 000/10 000 supports 1x nbre illimité supports	B7100AA/B7101AA B7102AA				
	Licence NDMP 1x To / 10x To /100 To	B7022BA/B7022DA/TD186AA				

*N° de produits (références) disponibles dans les « Spéc. rapides » sur hp.com Pour les versions électroniques, ajoutez E à la fin des références.

Figure 53 Structure de produit HP Data Protector

REMARQUE :

La structure de produit du présent manuel est uniquement proposée à des fins d'illustration. La toute dernière structure de produit officielle est disponible sur le Web, à l'adresse http://h18006.www1.hp.com/products/quickspecs/Division/Division.html#12647.

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.

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*.
- 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.

REMARQUE :

L'attribution de licences Data Protector (licences sur adresse IP, limitées ou permanentes, liées à l'adresse IP ou au sous-réseau, à l'exception des licences temporaires et des mots de passe d'urgence) suppose que le Gestionnaire de cellule possède une adresse IPv4. S'il est exécuté dans un environnement IPv6, le Gestionnaire de cellule doit être configuré en mode double pile, ce qui permet d'activer conjointement les protocoles IPv6 et IPv4. L'adresse IPv4 du Gestionnaire de cellule est utilisée à des fins d'attribution de licence.

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 IPv4.

- 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.

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 351 pour connaître la procédure à suivre pour contacter le Centre de remise de mot de passe HP.

Migration de licence vers Data Protector 6.20

Migrez directement vers Data Protector 6.20. Les licences des versions précédentes de Data Protector font l'objet d'une migration automatique.

Data Protector Les clients de Data Protector A.06.00, A.06.10 et A.06.11 sous contrat de support recevront gratuitement Data Protector 6.20. Une fois la mise à niveau de votre environnement vers Data Protector 6.20 effectuée, la fonctionnalité que vous utilisiez avec la version A.06.00, A.06.10 ou A.06.11 est disponible avec Data Protector 6.20 sans supplément de prix. Vous devez simplement acquérir de nouvelles licences si vous souhaitez vous procurer les nouvelles extensions fonctionnelles.

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 54 à la page 362.

L'outil de commande est disponible sur les DVD-ROM d'installation Data Protector.

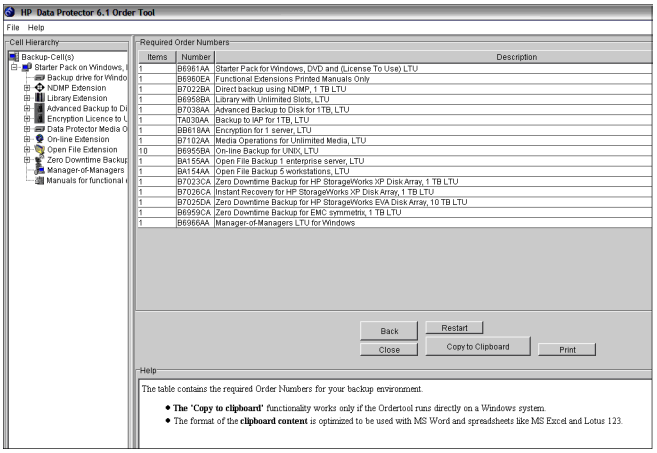


Figure 54 Exemple de résultats fournis par l'outil de commande Data Protector

Formulaires d'attribution de licences Data Protector

Cette section présente les formulaires d'attribution de licence Data Protector. Remplissez-les pour commander des mots de passe permanents à l'aide d'une des méthodes suivantes :

- Utilisez l'utilitaire HP AutoPass pour obtenir et installer les mots de passe permanents directement via Internet à partir du serveur Web du Centre de remise de mot de passe HP. Pour plus de détails, reportez-vous à la section "Obtention et installation de mots de passe permanents à l'aide de l'utilitaire HP AutoPass" à la page 348. Cette méthode est recommandée.
- 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.
- Imprimez la version électronique de ces formulaires de licence qui se trouve dans les fichiers suivants sur le système Gestionnaire de cellule et les supports de distribution :
  - HP-UX, Solaris et Linux : `/opt/omni/doc/C/license_forms_UNIX`
  - DVD-ROM Windows : `Nom_disque:Docs\license_forms.txt`

  ou utilisez les fichiers électroniques pour "copier" et "coller" votre message avant de l'adresser au *Centre de remise de mot de passe (PDC)*.

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	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, consultez l'aide en ligne.
Numéros de télécopie du *Centre de remise de mot de passe*	Pour obtenir les coordonnées, consultez 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*.

6 Résolution des problèmes d'installation

Dans ce chapitre

Ce chapitre contient des informations relatives aux problèmes d'installation. Vous trouverez des informations générales sur la résolution des problèmes dans le *Guide de dépannage HP Data Protector*.

Ce chapitre contient des informations sur les éléments suivants :

Problèmes de résolution de noms lors de l'installation du Gestionnaire de cellule Windows

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 369.

Problème

Le protocole TCP/IP n'est pas installé et configuré sur votre système.

Data Protector utilise le protocole TCP/IP pour les communications réseau ; celui-ci doit donc être installé et configuré sur chaque client de la cellule. Dans le cas contraire, l'installation est abandonnée.

Action

Vérifiez la configuration TCP/IP. Pour plus d'informations, reportez-vous à la section "Modification du numéro de port par défaut de Data Protector" à la page 414.

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, qui sont essentielles dans la cellule Data Protector :

- Du Gestionnaire de cellule vers tout autre membre de la cellule et inversement
- De l'Agent de support vers tout autre membre de la cellule et inversement

Utilisation de la commande omnicheck

Limites

- La commande vérifie uniquement les connexions entre membres de la cellule, et non les connexions DNS en général.

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 chaque Agent de support présent dans la cellule résolvent correctement les connexions DNS vers chaque client Data Protector de la cellule et inversement, exécutez la commande suivante :

  ```
  omnicheck -dns [-verbose]
  ```

- Pour vérifier qu'un client Data Protector particulier résout correctement les connexions DNS vers chaque client Data Protector de la cellule et inversement, 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 12 à la page 370 répertorie les messages retournés pour la commande `omnicheck`. Si le message renvoyé indique un problème de résolution DNS, reportez-vous au chapitre "Dépannage du réseau et de la communication" dans le Guide de dépannage HP Data Protector.

Tableau 12 Messages retournés

Message renvoyé	Signification
`client_1 ne peut pas se connecter à client_2`	Délai de connexion à *`client_2`* dépassé.
`client_1 se connecte à client_2, mais le système connecté se présente comme client_3`	Le fichier *`%SystemRoot%`*`\System32\drivers\etc\hosts/etc/hosts` (systèmes UNIX) sur le *`client_1`* n'est pas correctement configuré ou le nom d'hôte du *`client_2`* ne correspond pas à son nom DNS.

Message renvoyé	Signification
`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

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 6.20, Windows peut signaler que certaines applications ne sont pas installées ou qu'il est nécessaire de les réinstaller.

Ce problème est dû à une erreur de la procédure de mise à niveau de Microsoft Installer. Les données de la version 1.x de Microsoft Installer n'ont pas été transférées vers la version 2.x de Microsoft Installer que Data Protector installe sur l'ordinateur.

Action

Ce problème est décrit à l'article Q324906 de la base de connaissances Microsoft.

Problème

Gestionnaire de cellule Echec de l'installation d'un Gestionnaire de cellule sur un système Windows qui ne fait partie d'aucun domaine Windows

Le message d'erreur suivant s'affiche :

```
Impossible de faire correspondre le mot de passe et le nom
de compte spécifié.
```

Actions

Deux solutions possibles :

- Associer le système Windows sur lequel vous installez le Gestionnaire de cellule à un domaine.
- Utiliser le compte administrateur local pour le service CRS.

Problème

Le message d'erreur suivant s'affiche :

```
Fichier msvcr90.dll introuvable
```

Impossible de trouver la bibliothèque `MSVCR90.dll` (en majuscules) car seul le fichier `msvcr90.dll` (en minuscules) est disponible sur le partage réseau. Comme `MSVCR90.dll` et `msvcr90.dll` ne sont pas considérés comme un même fichier, `setup.exe` ne parvient pas à trouver le `dll` approprié.

Action

Renommez le fichier `msvcr90.dll` (minuscules) en `MSCVCR90.dll` (majuscules) ou reconfigurez le partage réseau de façon à ce qu'il ne soit plus sensible à la casse.

Problème

L'annulation de l'installation ne désinstalle pas des composants déjà installés

Si vous annulez l'installation de Data Protector alors que certains composants ont déjà été installés, Data Protector ne les désinstalle pas. L'installation se termine en affichant un message d'erreur.

Action

Désinstallez manuellement les composants déjà installés après avoir annulé l'installation.

Problèmes lors de l'installation à distance des clients Windows

Problème

Erreur lors du lancement du processus d'installation

Lorsque vous utilisez l'installation à distance Data Protector pour mettre à jour les clients Windows, le message d'erreur suivant s'affiche :

```
Erreur au démarrage du processus d'installation, err=[1326]
Accès réseau refusé : nom d'utilisateur inconnu ou mot de
passe incorrect.
```

Le problème est que le service `Inet Data Protector` fonctionne sur l'ordinateur distant sous un compte utilisateur qui ne dispose pas d'un accès au partage OmniBack sur l'ordinateur du Serveur d'installation. Il s'agit très probablement d'un utilisateur local.

Action

Remplacez l'utilisateur pour le service `Inet Data Protector` par un utilisateur qui puisse accéder au partage Data Protector.

Résolution des problèmes d'installation du Gestionnaire de cellule Data Protector sous Solaris

Problème

Impossible de créer un répertoire temporaire

Lors de l'installation de Gestionnaire de cellule sous Solaris, un répertoire temporaire ne peut être créé et l'installation échoue avec le message d'erreur suivant :

```
Processing package instance OB2-CORE from /tmp/
DP_A0611_SUN8.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 clients Solaris, la même quantité d'espace disque doit également être disponible dans le dossier /var/tmp.

Action

Vérifiez si vous disposez de suffisamment d'espace disque dans ces répertoires et redémarrez la procédure d'installation ou de mise à niveau.

Pour connaître l'espace disque nécessaire, reportez-vous au document *Références, notes de publication et annonces produits HP Data Protector*.

Problème

Problèmes d'installation d'un client HP-UX

Lorsque vous ajoutez un nouveau client HP-UX à une cellule Data Protector, le message d'erreur suivant s'affiche :

```
/tmp/omni_tmp/packet: vous ne disposez pas des autorisations
requises pour exécuter cette fonction SD...
```

```
Accès refusé à root pour démarrer l'agent sur le dépôt
enregistré /tmp/omni_tmp/packet. Insertion non autorisée sur
l'hôte.
```

Action

Arrêtez le démon `swagent` et relancez-le, soit en supprimant le processus, soit en le redémarrant à l'aide de la commande `/opt/omni/sbin/swagentd` ou `/opt/omni/sbin/swagentd -r`.

Vérifiez que vous disposez d'une entrée de bouclage local (localhost) dans le fichier hosts (`/etc/hosts`).

Problème

Problèmes d'installation d'un client Mac OS X

Lors de l'ajout d'un client Mac OS X à une cellule Data Protector, le processus `com.hp.omni` ne démarre pas.

Action

Sur Mac OS X, `launchd` permet de démarrer le processus `com.hp.omni`.

Pour démarrer le service, accédez à :

```
cd /usr/omni/newconfig/System/Library/LaunchDaemons
```

Exécutez la commande :

```
launchctl load com.hp.omni
```

Problème

Impossible de démarrer le processus Inet après l'installation du Gestionnaire de cellule UNIX Gestionnaire de cellule

Au démarrage du Gestionnaire de cellule, le message d'erreur suivant s'affiche :

```
ERREUR : Impossible de démarrer le service "omniinet", erreur
système : [1053] erreur inconnue 1053.
```

Action

Vérifiez que le service `inetd` ou `xinetd` est en cours d'exécution :

HP-UX et Solaris: `ps -ef | grep inetd`

Linux : `ps -ef | grep xinetd`

Pour démarrer le service, exécutez :

HP-UX : `/usr/sbin/inetd`

Solaris : `/usr/sbin/inetd -s`

Linux : `rcxinetd start`

Résolution des problèmes d'installation des clients Windows XP

Problème

Echec de l'installation à distance de clients Windows

Lorsqu'un système Windows XP est membre d'un groupe de travail et que la stratégie de sécurité Partage de fichiers simple est activée, les utilisateurs qui tentent d'accéder au système par le réseau sont obligés d'utiliser le compte Invité. Lors d'une installation à distance d'un client Data Protector, Data Protector demande à plusieurs reprises un nom d'utilisateur et un mot de passe valides car les droits de l'administrateur sont nécessaires pour l'installation à distance.

Action

Désactivez le partage de fichiers simple comme suit : Dans Windows XP, ouvrez l'**Explorateur Windows** ou **Poste de travail**, sélectionnez le menu **Outils**, cliquez sur l'option **Options des dossiers**, puis sur l'onglet **Affichage** et décochez l'option **Utiliser le partage de fichiers simple (recommandé)**.

La stratégie Partage de fichiers simple est ignorée :

- lorsque l'ordinateur est membre d'un domaine,
- lorsque le paramètre de stratégie de sécurité `Accès réseau : modèle de partage et de sécurité pour les comptes locaux` a la valeur `Classique : les utilisateurs locaux s'identifient eux-mêmes`

Résolution des problèmes d'installation des clients Windows Vista et Windows Server 2008

Problème

Echec de l'installation à distance de clients Windows

Echec de l'installation à distance d'un client Data Protector sur un système Windows Vista ou Windows Server 2008 avec le message d'erreur suivant :

```
[Normal] Connexion au client ordinateur.société.com...

[Normal] Terminé.

[Normal] Installation du service d'amorçage Data Protector
sur le client ordinateur.société.com...

[Critique] Impossible de se connecter au Gestionnaire de
contrôle des services sur le client ordinateur.société.com:
[5] Accès refusé.
```

Action

1. Sur le Serveur d'installation, exécutez la commande suivante pour indiquer un compte utilisateur du groupe local Administrateurs du système d'exploitation que le Serveur d'installation doit utiliser lors de l'installation à distance :

   ```
   omniinetpasswd -inst_srv_user utilisateur@domaine
   ```

   Notez que le compte utilisateur doit déjà être ajouté à la configuration Inet locale. Pour plus d'informations, reportez-vous à la description de la commande `omniinetpasswd` dans le *Guide de référence de l'interface de ligne de commande HP Data Protector*.
2. Relancez l'installation à distance du client Data Protector.

Vérification de l'installation du client Data Protector

La vérification de l'installation du client Data Protector se divise en plusieurs étapes :

- Vérification de la configuration DNS des systèmes Gestionnaire 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.

Pour vérifier une installation Data Protector à l'aide de l'interface utilisateur 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 382.

Pour plus d'informations sur la vérification de l'installation sur les systèmes UNIX à l'aide de l'interface en ligne de commande de Data Protector, reportez-vous à la page `ob2install` du manuel.

Résolution des problèmes de la mise à niveau

Problème

Les fichiers de la base de données IDB et de configuration ne sont plus disponibles après la mise à niveau

Après la mise à niveau du Gestionnaire de cellule à partir d'une version précédente, la base IDB ainsi que tous les fichiers de configuration ne sont pas disponibles. Ce problème survient en cas d'interruption de la procédure de mise à niveau, quelle qu'en soit la raison.

Action

Restaurez Data Protector à partir de la sauvegarde effectuée avant la mise à niveau, éliminez la raison de l'interruption et redémarrez la mise à niveau.

Problème

Les anciens correctifs Data Protector ne sont pas supprimés après la mise à niveau

Les anciens correctifs Data Protector sont répertoriés dans la liste des programmes installés si vous exécutez la commande `swlist` une fois la mise à niveau Data Protector terminée. Les correctifs ont été supprimés du système au cours de la mise à niveau, mais restent dans la base de données sw.

Pour savoir quels correctifs Data Protector sont installés, reportez-vous à la section "Contrôle des correctifs Data Protector installés" à la page 250.

Action

Pour supprimer les anciens correctifs de la base de données sw, exécutez la commande suivante :

`swmodify -u` *`correctif`*`.\*` *`correctif`*

Par exemple, pour supprimer le correctif "`PHSS_30143`" de la base de données sw, exécutez la commande suivante :

```
swmodify -u PHSS_30143.\* PHSS_30143
```

Problème

La taille maximale des fichiers de base de données dépasse 2 Go

Sous HP-UX 11.23 et 11.31 (Itanium) et sous SuSE Linux (x86-64), la taille maximale des fichiers de base de données (`dirs.dat`, `fnames.dat`, `fn?.ext` et leurs fichiers d'extension) peut dépasser la taille maximale par défaut de 2 Go. Par conséquent, lors d'une mise à niveau vers Data Protector 6.20, un message d'avertissement s'affiche pour inviter à régler la taille maximale des fichiers de base de données :

```
Exécutez omnidbutil -modifytblspace pour régler la taille
maximale des fichiers de base de données.
```

Action

Vous devez effectuer cette opération après la mise à niveau, car la procédure de réglage de la taille maximale des fichiers de base de données peut s'avérer gourmande en temps et en espace, selon la taille de la base de données. Tant que

le réglage n'est pas effectué, Data Protector 6.20 signale des tailles d'espace de table incorrectes comme c'est le cas dans la version A.06.00. Toutefois, il reste possible d'exécuter une sauvegarde et une restauration.

REMARQUE :

Vérifiez que l'espace disque disponible est suffisant avant de lancer le réglage. Vous avez besoin d'un espace disponible supplémentaire au moins égal à la taille actuelle de la base de données que vous allez exporter.

Prévoyez un temps suffisant pour l'ensemble de l'opération. L'exportation et l'importation de la base de données peuvent prendre beaucoup de temps (jusqu'à plusieurs jours, selon la complexité et la taille de la base de données) et vous ne pouvez pas effectuer de sauvegarde ou de restauration pendant l'exportation et l'importation.

Pour résoudre le problème, procédez comme suit :

1. Effectuez une sauvegarde réussie de l'ensemble de l'IDB.
2. Exportez l'IDB dans un répertoire temporaire existant :

   ```
   omnidbutil -writedb -mmdb répertoireMMDB -cdb répertoireCDB
   ```

   où *répertoireCDB* et *répertoireMMDB* sont des répertoires temporaires vers lesquels les éléments CDB et MMDB sont exportés.
3. Initialisez l'IDB :

   ```
   omnidbinit
   ```
4. Ajoutez le nombre requis de fichiers d'extension pour le fichier d'espace de table :

   ```
   omnidbutil -extendtblspace nom_fichier_espace_table
   nom_chemin -maxsize taille_mo
   ```

   Par exemple, si la taille du fichier `fnames.dat` est de 7 Go, vous devez ajouter trois fichiers d'extension avec une taille maximale de 2047 Mo en exécutant la même commande trois fois :

   ```
   omnidbutil -extendtblspace fnames.dat /var/opt/omni/server/
   db40/datafiles/cdb -maxsize 2047
   omnidbutil -extendtblspace fnames.dat /var/opt/omni/server/
   db40/datafiles/cdb -maxsize 2047
   omnidbutil -extendtblspace fnames.dat /var/opt/omni/server/
   db40/datafiles/cdb -maxsize 2047
   ```

Ces commandes créent trois fichiers d'extension, `fnames.dat1`, `fnames.dat2` et `fnames.dat3`.

5. Réglez la taille maximale des fichiers de base de données existants :

   ```
   omnidbutil –modifytblspace
   ```

   Suivant l'exemple ci-dessus, `fnames.dat`, qui atteignait auparavant une taille de 7 Go, est maintenant limité à 2 Go.

6. Importez l'IDB :

   ```
   omnidbutil -readdb -mmdb répertoireMMDB -cdb répertoireCDB
   ```

   Si vous n'avez pas créé un nombre suffisant de fichiers d'extension, la commande `omnidbutil` se termine avec le message suivant :

   ```
   Mémoire insuffisante pour l'espace de table
   nom_espace_table.
   ```

   Ajoutez le nombre requis de fichiers d'extension et relancez l'opération d'importation.

7. Une fois le réglage réussi, supprimez les fichiers temporaires.

Problème

La mise à niveau d'un client Agent de support utilisant la bibliothèque StorageTek engendre des problèmes de connectivité

Après la mise à niveau du composant Agent de support Data Protector sur un système qui utilise la bibliothèque StorageTek, la connexion avec la bibliothèque est perdue et les sessions Data Protector impliquant cette bibliothèque peuvent cesser de répondre ou s'arrêter de façon anormale.

Action

Le redémarrage du service ou démon prenant en charge la bibliothèque StorageTek peut permettre de résoudre le problème :

Systèmes Windows : Au moyen de l'outil d'administration Services, redémarrez le service `LibAttach`.

Systèmes HP-UX et Solaris : Exécutez les commandes `/opt/omni/acs/ssi.sh stop` et `/opt/omni/acs/ssi.sh start nom_hôte_ACSLS`, où *`nom_hôte_ACSLS`* est le nom du système sur lequel le logiciel de la bibliothèque ACS (Automated Cartridge System - système de cartouche automatisé) est installé.

Systèmes AIX : Exécutez les commandes `/usr/omni/acs/ssi.sh stop` et `/usr/omni/acs/ssi.sh start nom_hôte_ACSLS`, où *`nom_hôte_ACSLS`* est le nom

du système sur lequel le logiciel de la bibliothèque ACS (Automated Cartridge System - système de cartouche automatisé) est installé.

Procédure de mise à niveau manuelle

Normalement, vous mettez à niveau Data Protector A.06.00, A.06.10 ou A.06.11 sur le Gestionnaire de cellule UNIX et le Serveur d'installation en exécutant la commande `omnisetup.sh`, qui exécute une procédure de mise à niveau automatique. Il est toutefois possible d'effectuer une mise à niveau manuelle. Reportez-vous à la section "Mise à niveau sur des systèmes HP-UX, Solaris et Linux à l'aide d'outils natifs" à la page 406.

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 :

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 ou Linux :

`/var/opt/omni/log/debug.log`

Client Windows (le système sur lequel tourne le programme d'installation) :

- `Temp\SetupLog.log`
- `Temp\OB2DBG_did__setup_Hôte_num_débogage_setup.txt` (pour plus d'informations)

où :

- `did` (ID de débogage) est l'ID de processus du premier processus acceptant les paramètres de débogage. Cet ID est également l'ID de la session de débogage. Tous les autres processus utiliseront cet ID.
- *`Hôte`* est le nom de l'hôte sur lequel le fichier de trace est créé.
- *`num_débogage`* est un numéro généré par Data Protector.

- `Temp\CLUS_DBG_num_débogage.TXT` (dans les environnements de clusters)

L'emplacement du répertoire `Temp` est spécifié par la variable d'environnement `TEMP`. Pour connaître la valeur de cette variable, exécutez la commande `set`.

Installation distante

Si vous rencontrez des difficultés lors d'une installation à distance, reportez-vous aux fichiers journaux suivants :

Serveur d'installation UNIX :

`/var/opt/omni/log/IS_install.log`

Client Windows (système distant sur lequel les composants doivent être installés) :

- `SystemRoot\TEMP\OB2DBG_did_INSTALL_SERVICE_num_débogage_debug.txt`
- `SystemRoot\TEMP\CLUS_DBG_num_débogage.TXT`

L'emplacement du répertoire `Temp` est spécifié par la variable d'environnement `TEMP` et `SystemRoot` est un chemin spécifié dans la variable d'environnement `SystemRoot`.

Si les fichiers journaux n'ont pas été créés, exécutez l'installation à distance avec l'option de débogage. Reportez-vous à la section “Création de traces d'exécution de l'installation” à la page 384.

Fichiers journaux Data Protector

Les fichiers journaux Data Protector répertoriés ci-dessous se trouvent dans :

Windows Vista, Windows Server 2008 : `données_programme_Data_Protector\log`

Autres systèmes Windows : `répertoire_Data_Protector\log`

HP-UX, Solaris et Linux : `/var/opt/omni/log` et `/var/opt/omni/server/log`

Autres systèmes UNIX et Mac OS X : `/usr/omni/log`

Novell NetWare : `SYS:\USR\OMNI\LOG`

Les fichiers journaux suivants sont importants pour la résolution des problèmes d'installation :

`debug.log`	Contient des conditions inattendues. Bien que certaines pourront vous servir, ces informations sont surtout destinées au service de support.
`inet.log`	Contient des demandes effectuées auprès du service `inet` Data Protector. Il peut être utile pour contrôler les dernières activités de Data Protector sur les clients.
`IS_install.log`	Contient une trace d'installation à distance et se trouve sur le Serveur d'installation.
`omnisv.log`	Contient des informations relatives au démarrage et à l'arrêt des services Data Protector.
`upgrade.log`	Ce journal est créé lors de la mise à niveau et contient des messages relatifs à la mise à niveau de la partie centrale (UCP) et à la mise à niveau de la partie concernant les détails (UDP).
`OB2_Upgrade.log`	Ce fichier, créé lors de la mise à niveau, contient les traces de la procédure de celle-ci.

Pour obtenir des informations sur d'autres fichiers journaux, reportez-vous au *Guide de dépannage HP Data Protector*.

Création de traces d'exécution de l'installation

Exécutez l'installation avec l'option `debug` si le service support clientèle HP vous le demande. Pour plus d'informations sur le débogage, notamment sur les options de débogage ci-dessous, et sur la préparation des données à envoyer au service support clientèle HP, reportez-vous au *Guide de dépannage HP Data Protector*.

Windows :

Pour déboguer une installation à distance sur un système Windows, exécutez l'interface utilisateur graphique 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 :

  `données_programme_Data_Protector\tmp\OB2DBG_did__BM_NomHôte_NumDébogage_SuffixeDébogage` (Windows Server 2008)

  `répertoire_Data_Protector\tmp\OB2DBG_did__BM_NomHôte_NumDébogage_SuffixeDébogage` (autres systèmes Windows)

- Sur le système distant :

  `SystemRoot:\Temp\OB2DBG_did__INSTALL_SERVICE_NomHôte_N°Débogage_SuffixeDébogage`

UNIX :

Pour procéder au débogage de l'installation sur un système UNIX, exécutez l'interface utilisateur graphique de Data Protector en utilisant l'option de débogage :

```
xomni -debug 1-99 Suffixe_débogage
```

ou

```
xomniadmin -debug 1-99 Suffixe_débogage
```

Une fois la session terminée/abandonnée, récupérez les résultats du débogage dans le répertoire `tmp` du système Serveur d'installation.

A Installation et mise à niveau de Data Protector à l'aide d'outils UNIX natifs

Dans cette annexe

Cette annexe explique comment installer et mettre à niveau Data Protector sur des systèmes UNIX, à l'aide des outils d'installation natifs — `swinstall` sous HP-UX, `pkgadd` sous Solaris et `rpm` sous Linux.

REMARQUE :

Pour installer ou mettre à niveau Data Protector, la méthode recommandée consiste à utiliser le script `omnisetup.sh`. Reportez-vous aux sections "Installation d'un Gestionnaire de cellule UNIX" à la page 45 et "Mise à niveau du Gestionnaire de cellule et du Serveur d'installation UNIX" à la page 278.

Installation sur des systèmes HP-UX, Solaris et Linux à l'aide d'outils natifs

REMARQUE :

Les procédures d'installation natives sous 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

Pour installer le Gestionnaire de cellule UNIX sur un système HP-UX, procédez comme suit :

1. Insérez et montez le DVD-ROM d'installation HP-UX et exécutez l'utilitaire `/usr/sbin/swinstall`.
2. Dans la fenêtre Spécifier source, sélectionnez **Répertoire réseau/CD-ROM**, puis saisissez `Point_de_montage/hpux/DP_DEPOT` dans la zone **Chemin d'accès au dépôt source**. Cliquez 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`.

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, double-cliquez 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.

   Ce produit contient les sous-produits suivants :

OB2-CM	Logiciel Gestionnaire de cellule
OB2-DOCS	Documentation de Data Protector comprenant les guides Data Protector au format PDF et l'aide en ligne (WebHelp)
OB2-IS	Serveur d'installation Data Protector

   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 55 à la page 390.

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.

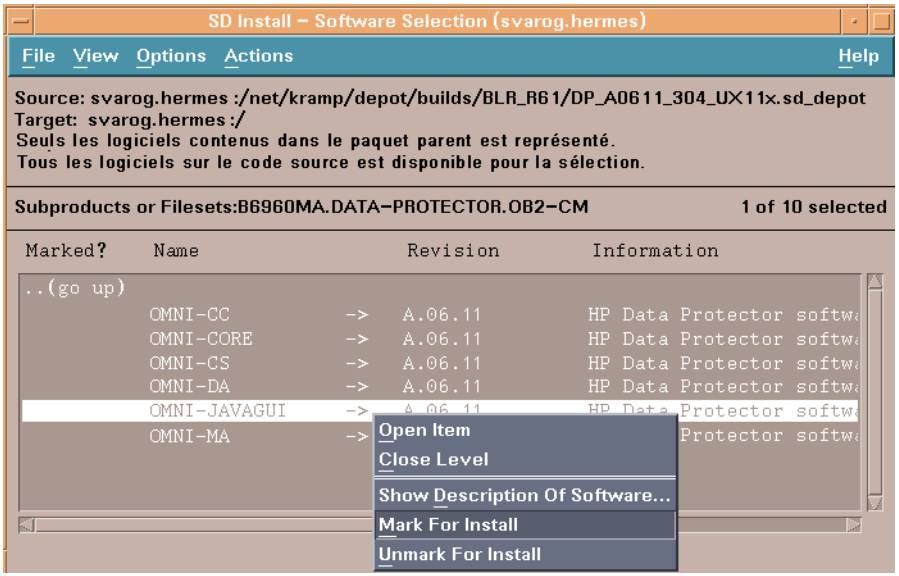


Figure 55 Fenêtre Installation SD - Sélection de logiciel

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.

REMARQUE :

Pour installer des logiciels à partir d'un périphérique à bandes 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, procédez comme suit :

1. Insérez le DVD-ROM d'installation Solaris et Linux.
2. Accédez au répertoire principal *source_package*, c'est-à-dire au répertoire contenant le fichier dépôt d'installation (dans ce cas, `Point_de_montage/solaris/DP_DEPOT`).

3. Utilisez l'outil `pkgadd` pour installer les packages Data Protector :

   ```
   pkgadd -d 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 de ligne de commande.
OB2-CS	Logiciel du Gestionnaire de cellule.
OB2-DA	Logiciel Agent de disque. Ce logiciel est requis ; il est indispensable pour sauvegarder la base de données IDB.

   et (facultatif) :

OB2-MA	Logiciel Agent général de support. Ce logiciel est requis si vous souhaitez connecter un périphérique de sauvegarde au Gestionnaire de cellule.
OB2-DOCS	Documentation de Data Protector comprenant les guides Data Protector au format PDF et l'aide en ligne (WebHelp).
OB2-JAVAGUI	Interface utilisateur graphique compatible Java. Elle contient l'interface utilisateur du Gestionnaire de cellule et l'interface utilisateur du MoM (Manager-of-Managers). Pour installer l'interface de ligne de commande sur un client disposant de l'interface utilisateur graphique Java, vous devez installer le package OB2-CC.

IMPORTANT :

Les packages de sous-produits sous Solaris 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
```

REMARQUE :

Si vous avez installé le Gestionnaire de cellule sous Solaris 9 ou Solaris 10, installez l'Agent de disque à distance sur le Serveur d'installation à l'aide d'un Gestionnaire de cellule. L'Agent de disque Solaris générique sera ainsi remplacé par l'Agent de disque Solaris 9 ou Solaris 10. Sous Solaris 10, l'installation à distance de l'Agent de support sur le Gestionnaire de cellule s'avère également nécessaire. Reportez-vous à la section “Installation distante de clients Data Protector” à la page 83 ou à la page de manuel `ob2install`.

Installation du Gestionnaire de cellule sur des systèmes Linux à l'aide de rpm

Pour installer le Gestionnaire de cellule sur un système Linux, procédez comme suit :

1. Insérez et montez le DVD-ROM d'installation Solaris et Linux.
2. Accédez au répertoire `linux_x86_64/DP_DEPOT`.

3. Pour installer un package, exécutez la commande ci-dessous :

   ```
   rpm -i nom_package-A.06.20-1.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.
OB2-MA	Logiciel Agent général de support. Ce logiciel est requis si vous souhaitez connecter un périphérique de sauvegarde au Gestionnaire de cellule.
OB2-DOCS	Documentation de Data Protector comprenant les guides Data Protector au format PDF et l'aide en ligne (WebHelp).
OB2-JAVAGUI	Interface utilisateur graphique compatible Java. Elle contient l'interface utilisateur du Gestionnaire de cellule et l'interface utilisateur du MoM (Manager-of-Managers). Pour installer l'interface de ligne de commande sur un client disposant de l'interface utilisateur

graphique Java, vous devez installer le package OB2-CC.

IMPORTANT :

Les packages de sous-produits sous Linux sont interdépendants. Vous devez installer ces packages en respectant l'ordre de la liste ci-dessus.

4. Redémarrez les services Data Protector :

```
/opt/omni/sbin/omnisv stop
/opt/omni/sbin/omnisv start
```

Installation d'un Serveur d'installation sur un système HP-UX à l'aide de swinstall

1. Insérez et montez le DVD-ROM d'installation HP-UX et exécutez l'utilitaire `/usr/sbin/swinstall`.
2. Dans la fenêtre Spécifier source, sélectionnez **Répertoire réseau/CD-ROM**, puis saisissez `Point_de_montage/hpux/DP_DEPOT` dans la zone **Chemin d'accès au dépôt source**. Cliquez 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 guides Data Protector au format PDF et l'aide en ligne (WebHelp).
OB2-IS	Serveur d'installation Data Protector

4. Dans la fenêtre Installation SD - Sélection de logiciel, double-cliquez sur **DATA-PROTECTOR** pour afficher la liste des logiciels en vue de l'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 HP-UX.

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 Solaris et Linux.

2. Accédez au répertoire principal *source_package*, c'est-à-dire au 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 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-CFP	Paquets d'installation principale du Serveur d'installation communs à toutes les plates-formes UNIX.
OB2-CCP	Paquets d'installation à distance de la console de cellule pour tous les systèmes UNIX.
OB2-DAP	Paquets d'installation à distance de l'Agent de disque pour tous les systèmes UNIX.
OB2-MAP	Paquets d'installation à distance de l'Agent de support pour tous les systèmes UNIX.

   De plus, si vous configurez un Serveur d'installation indépendant (c'est-à-dire ne figurant pas dans le Gestionnaire de cellule) et souhaitez utiliser l'interface utilisateur :

OB2-CC	Logiciel de la console de cellule. Ce logiciel contient l'interface de ligne de commande.
OB2-JAVAGUI	Logiciel de l'interface Java. Il contient l'interface utilisateur du Gestionnaire de cellule et l'interface utilisateur du MoM (Manager-of-Managers).

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 nom_du_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 d'installation à distance 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-JGUIP	Paquet d'installation à distance de l'interface utilisateur Java. Ce paquet contient l'interface utilisateur du Gestionnaire de cellule et l'interface utilisateur du MoM (Manager-of-Managers). Pour installer l'interface de ligne de commande sur un client disposant de l'interface utilisateur Java, vous devez installer le package OB2-CC.
OB2-SAPP	Composant d'intégration SAP.
OB2-VMWP	Composant d'intégration VMware.
OB2-SAPDBP	Composant d'intégration SAP DB.
OB2-INFP	Composant d'intégration Informix.
OB2-LOTP	Composant d'intégration Lotus Notes/Domino.
OB2-SYBP	Composant d'intégration Sybase.
OB2-OR8P	Composant d'intégration Oracle.
OB2-DB2P	Composant d'intégration DB2.
OB2-EMCP	Composant d'intégration EMC Symmetrix.
OB2-SMISP	Composant Agent HP StorageWorks P6000 EVA SMI-S.
OB2-SSEAP	Composant Agent HP StorageWorks P9000 XP.
OB2-NDMPP	Logiciel Agent de support NDMP.

OB2-OVP	Composant d'intégration HP NNM.
OB2-FRAP	Package de documentation en français (guides, aide).
OB2-JPNP	Package de documentation en japonais (guides, aide).
OB2-CHSP	Package de documentation en chinois simplifié (guides, aide).
OB2-PEGP	Package PEGASUS.
OB2-VLSAMP	Package VLS-AM.

Pour obtenir la liste complète des composants et dépendances relatives à l'installation, reportez-vous au Tableau 9 à la page 271.

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 Solaris et Linux.

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 utilisateur graphique 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 54.

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

Etape suivante

A ce stade de la procédure, les serveurs d'installation pour UNIX doivent être installés sur votre réseau. Vous devez maintenant effectuer les tâches suivantes :

1. Si vous avez configuré un Serveur d'installation indépendant (ne figurant pas dans le Gestionnaire de cellule), vous devez 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 224.

   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 d'installation à distance installés. Ce fichier peut être utilisé à partir de l'interface de ligne de commande pour vérifier les paquets d'installation à distance disponibles. Pour maintenir ce fichier à jour, vous devrez exporter, puis réimporter un Serveur d'installation à chaque installation ou suppression d'un paquet d'installation à distance. Cette procédure est valable même dans le cas où un Serveur d'installation est installé sur le même système que le Gestionnaire de cellule.

2. Installez le Serveur d'installation pour Windows si vous disposez de systèmes Windows dans votre cellule Data Protector. Reportez-vous à la section Configuration système requise à la page 68.
3. Distribuez le logiciel aux clients. Reportez-vous à la section "Installation des clients Data Protector" à la page 72.

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 Solaris et Linux.
2. Accédez au répertoire contenant le fichier d'archives d'installation (dans ce cas, `Point_de_montage/linux_x86_64/DP_DEPOT`).

3. Pour chaque package, exécutez la commande suivante :

   ```
   rpm -i nom_package-A.06.20-1.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-CFP	Logiciel Serveur d'installation principal commun à toutes les plates-formes UNIX.
OB2-CCP	Paquets d'installation à distance de la console de cellule pour tous les systèmes UNIX.
OB2-DAP	Paquets d'installation à distance de l'Agent de disque pour tous les systèmes UNIX.
OB2-MAP	Paquets d'installation à distance de l'Agent de support pour tous les systèmes UNIX.

   De plus, si vous configurez un Serveur d'installation indépendant (c'est-à-dire ne figurant pas dans le Gestionnaire de cellule) et souhaitez utiliser l'interface utilisateur :

OB2-CC	Logiciel de la console de cellule. Ce logiciel contient l'interface de ligne de commande.
OB2-JAVAGUI	Logiciel de l'interface Java. Il contient l'interface utilisateur du Gestionnaire de cellule et l'interface utilisateur du MoM (Manager-of-Managers).

4. Une fois ces composants installés, utilisez `rpm` pour installer les paquets d'installation à distance 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-JGUIP	Paquet d'installation à distance de l'interface utilisateur Java. Ce paquet contient l'interface utilisateur du Gestionnaire de cellule et l'interface utilisateur du MoM (Manager-of-Managers). Pour installer l'interface de ligne de commande sur un client disposant de l'interface utilisateur Java, vous devez installer le package OB2-CC.
OB2-SAPP	Composant d'intégration SAP.
OB2-VMWP	Composant d'intégration VMware.
OB2-SAPDBP	Composant d'intégration SAP DB.
OB2-INFP	Composant d'intégration Informix.
OB2-LOTP	Composant d'intégration Lotus Notes/Domino.
OB2-SYBP	Composant d'intégration Sybase.
OB2-OR8P	Composant d'intégration Oracle.
OB2-DB2P	Composant d'intégration DB2.
OB2-EMCP	Composant d'intégration EMC Symmetrix.
OB2-SMISAP	Composant Agent HP StorageWorks P6000 EVA SMI-S.
OB2-SSEAP	Composant Agent HP StorageWorks P9000 XP.
OB2-NDMPP	Logiciel Agent de support NDMP.

OB2-OVP	Composant d'intégration HP NNM.
OB2-FRAP	Package de documentation en français (guides, aide).
OB2-JPNP	Package de documentation en japonais (guides, aide).
OB2-CHSP	Package de documentation en chinois simplifié (guides, aide).
OB2-DOCSP	Package de documentation en anglais (guides, aide).
OB2-PEGP	Package PEGASUS.
OB2-VLSAMP	Package VLS-AM.

Pour obtenir la liste complète des packages d'installation et dépendances associées, reportez-vous au Tableau 10 à la page 271.

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 Solaris et Linux.

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 (ne figurant pas dans le Gestionnaire de cellule), vous devez 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 224.

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 d'installation à distance installés. Ce fichier peut être utilisé à partir de l'interface de ligne de commande pour vérifier les paquets d'installation à distance disponibles. Pour maintenir ce fichier à jour, vous devrez exporter, puis réimporter un Serveur d'installation à chaque installation ou suppression d'un paquet d'installation à distance. Cette procédure est valable même dans le cas où un Serveur d'installation est installé sur le même système que le Gestionnaire de cellule.

2. Installez le Serveur d'installation pour Windows si vous disposez de systèmes Windows dans votre cellule Data Protector. Reportez-vous à la section Configuration système requise à la page 68.
3. Distribuez le logiciel aux clients. Reportez-vous à la section “Installation des clients Data Protector” à la page 72.

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 installant à distance 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 72.

Mise à niveau sur des systèmes HP-UX, Solaris et Linux à l'aide d'outils natifs

Mise à niveau de Data Protector sur les systèmes HP-UX à l'aide de swinstall

Une mise à niveau du Gestionnaire de cellule doit être réalisée à partir du DVD-ROM d'installation HP-UX.

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 installant à distance les composants d'installation à partir du Serveur d'installation. Pour plus de détails, reportez-vous à la section "Installation en local de clients UNIX et Mac OS X" à la page 151 ou "Installation distante de clients Data Protector" à la page 83.

Procédure de mise à niveau

Pour mettre à niveau Data Protector A.06.00, A.06.10 ou A.06.11 vers Data Protector 6.20, à l'aide de `swinstall`, procédez comme suit :

1. Connectez-vous en tant que `root` et arrêtez les services Data Protector sur le Gestionnaire de cellule en exécutant la commande `/opt/omni/sbin/omnisv -stop`.

   Tapez `ps -ef | grep omni` pour vérifier si tous les services ont bien été arrêtés. Aucun service Data Protector ne doit être répertorié sur exécution de la commande `ps -ef | grep omni`.

2. Pour mettre à niveau un Gestionnaire de cellule et/ou un Serveur d'installation, suivez les procédures décrites dans la section "Installation d'un Gestionnaire de cellule sur un système HP-UX à l'aide de swinstall" à la page 388 et/ou la section "Installation d'un Serveur d'installation sur un système HP-UX à l'aide de swinstall" à la page 394.

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 installant à distance les composants d'installation à partir du Serveur d'installation. Pour plus de détails, reportez-vous à la section “Installation en local de clients UNIX et Mac OS X” à la page 151 ou “Installation distante de clients Data Protector” à la page 83.

Procédure de mise à niveau

Pour mettre à niveau Data Protector A.06.00, A.06.10 ou A.06.11 vers Data Protector 6.20, à l'aide de `pkgadd`, procédez comme suit :

1. Connectez-vous en tant que `root` et arrêtez les services Data Protector sur le Gestionnaire de cellule en exécutant la commande `/opt/omni/sbin/omnisv -stop`.

   Tapez `ps -ef | grep omni` pour vérifier si tous les services ont bien été arrêtés. Aucun service Data Protector ne doit être répertorié sur exécution de la commande `ps -ef | grep omni`.

2. Désinstallez Data Protector à l'aide de `pkgrm`.

   Les fichiers de configuration et la base de données sont préservés durant cette procédure.

3. Exécutez la commande `pkginfo` pour vérifier que vous avez bien désinstallé l'ancienne version de Data Protector. Les anciennes versions de Data Protector ne doivent pas figurer dans la liste.

   Assurez-vous que la base de données et les fichiers de configuration sont toujours présents. Les répertoires suivants doivent toujours exister et contenir les fichiers binaires :

   - `/opt/omni`
   - `/var/opt/omni`
   - `/etc/opt/omni`

4. Si vous mettez à niveau le Gestionnaire de cellule, insérez et montez le DVD-ROM d'installation Solaris et Linux, puis 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 390.

   Si vous mettez à niveau le Serveur d'installation, insérez et montez le DVD-ROM d'installation Solaris et Linux, puis 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 395.

REMARQUE :

Si vous avez mis à niveau le Gestionnaire de cellule sous Solaris 9 ou Solaris 10, installez l'Agent de disque à distance sur le Gestionnaire de cellule après la mise à niveau à l'aide d'un Serveur d'installation. L'Agent de disque Solaris générique sera ainsi remplacé par l'Agent de disque Solaris 9 ou Solaris 10. Sous Solaris 10, l'installation à distance de l'Agent de support sur le Gestionnaire de cellule s'avère également nécessaire. Reportez-vous à la section "Installation distante de clients Data Protector à la page 83 ou à la page de manuel `ob2install`.

Mise à niveau de Data Protector sur des systèmes Linux à l'aide de rpm

Pour mettre à niveau le Gestionnaire de cellule ou le Serveur d'installation de Linux, désinstallez l'ancienne version et installez la nouvelle version du produit.

Les composants du client installés sur le système Gestionnaire de cellule ne sont *pas* mis à niveau en même temps que Gestionnaire de cellule ; ils doivent être mis à

niveau en chargeant `omnisetup.sh` ou en installant à distance les composants d'installation à partir du Serveur d'installation. Pour plus de détails, reportez-vous à la section “Installation en local de clients UNIX et Mac OS X” à la page 151 ou “Installation distante de clients Data Protector” à la page 83.

Procédure de mise à niveau

Pour mettre à niveau Data Protector A.06.00, A.06.10 ou A.06.11 vers Data Protector 6.20, à l'aide de `rpm`, procédez comme suit :

1. Connectez-vous en tant que `root` et arrêtez les services Data Protector sur le Gestionnaire de cellule en exécutant la commande `/opt/omni/sbin/omnisv -stop`.

   Tapez `ps -ef | grep omni` pour vérifier si tous les services ont bien été arrêtés. Aucun service Data Protector ne doit être répertorié sur exécution de la commande `ps -ef | grep omni`.

2. Désinstallez Data Protector à l'aide de `rpm`.

   Les fichiers de configuration et la base de données sont préservés durant cette procédure.

3. Exécutez la commande `rpm–q` pour vérifier que vous avez bien désinstallé l'ancienne version de Data Protector. Les anciennes versions de Data Protector ne doivent pas figurer dans la liste.

   Assurez-vous que la base de données et les fichiers de configuration sont toujours présents. Les répertoires suivants doivent toujours exister et contenir les fichiers binaires :

   - `/opt/omni`
   - `/var/opt/omni`
   - `/etc/opt/omni`

4. Si vous mettez à niveau le Gestionnaire de cellule, insérez et montez le DVD-ROM d'installation Solaris et Linux, puis utilisez `rpm` pour installer le Gestionnaire de cellule. Pour obtenir des informations détaillées sur la procédure à suivre, reportez-vous à la section Installation du Gestionnaire de cellule sur des systèmes Linux à l'aide de rpm.

   Si vous mettez à niveau le Serveur d'installation, insérez et montez le DVD-ROM d'installation Solaris et Linux, puis installez le Serveur d'installation. Pour obtenir des informations détaillées sur la procédure à suivre, reportez-vous à la section Installation d'un Serveur d'installation sur des systèmes Linux à l'aide de rpm.

B Tâches de préparation et de maintenance du système

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. Il s'agit notamment des tâches de préparation et de maintenance du système.

Configuration réseau sur les systèmes UNIX

Lorsque vous installez Data Protector sur un système UNIX, Data Protector `Inet` est enregistré en tant que service réseau. En règle générale, ceci implique les étapes suivantes :

- Modification du fichier `/etc/services` pour la définition d'un port d'écoute dédié au service Data Protector `Inet`.
- Enregistrement du service Data Protector `Inet` dans le démon `inetd` du système ou son équivalent (`xinetd`, `launchd`).

Lorsque vous modifiez une configuration réseau, il peut arriver que la configuration initiale du service Data Protector `Inet` devienne incomplète ou non valide. Ceci peut notamment se produire lors de l'ajout ou de la suppression d'interfaces réseau IPv6, en raison des paramètres spécifiques du système pour l'ajout de la prise en charge d'IPv6 dans les services réseau.

Pour mettre à jour la configuration du service Data Protector `Inet`, vous disposez de l'utilitaire `dpsvcsetup.sh`. Egalement utilisé lors de l'installation, cet utilitaire, qui recueille les informations nécessaires et met à jour la configuration du système en conséquence, se trouve dans le répertoire `/opt/omni/sbin` ou `/usr/omni/bin` selon le système d'exploitation.

- Pour mettre à jour la configuration de Data Protector `Inet`, exécutez la commande suivante :

  `dpsvcsetup.sh -update`.
- Pour enregistrer le service Data Protector `Inet` en tant que service réseau, exécutez la commande suivante :

  `dpsvcsetup.sh -install`.
- Pour annuler l'enregistrement du service Data Protector `Inet` en tant que service réseau, exécutez la commande suivante :

  `dpsvcsetup.sh -uninstall`.

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. Tous les systèmes du réseau doivent être capables de résoudre l'adresse du Gestionnaire de cellule ainsi que de tous les clients équipés d'Agents de support et de périphériques de supports physiques. Le Gestionnaire de cellule doit être capable de résoudre les noms de tous les clients de la cellule.

Une fois que vous avez installé le protocole TCP/IP, vous pouvez vérifier sa configuration à l'aide des commandes `ping` et `ipconfig/ifconfig`.

Sur certains systèmes, la commande `ping` ne peut être utilisée pour les adresses IPv6 et doit être remplacée par la commande `ping6`.

1. Dans la ligne de commande, exécutez la commande suivante :

   Systèmes Windows : `ipconfig /all`

   Systèmes UNIX : `ifconfig` *`interface`* ou `ifconfig -a` ou `nestat -i`, selon le système

   Des informations précises sur votre configuration TCP/IP ainsi que sur les adresses définies pour votre carte réseau s'affichent. 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 `ordinateur` et le nom de domaine `entreprise.com`, vous devez taper : `ping ordinateur.entreprise.com`.

   Si cela ne fonctionne pas, vérifiez si le nom de domaine indiqué dans la fenêtre des propriétés TCP/IP est correct. Contrôlez également le fichier hosts et le DNS. Assurez-vous que la résolution du nom pour le Gestionnaire de cellule et les clients fonctionne dans les deux sens :

   - Sur le Gestionnaire de cellule, vous devez être en mesure de sonder (faire un ping vers) chaque client.
   - Sur les clients, vous devez être en mesure de sonder (faire un ping vers) le Gestionnaire de cellule et chaque client doté d'un Agent de support.

REMARQUE :

Notez que, lors de l'utilisation du fichier de l'hôte pour la résolution du nom, le test ci-dessus ne garantit pas le fonctionnement de la résolution du nom. Dans ce cas, vous voudrez peut-être utiliser **l'outil de vérification DNS** une fois Data Protector installé.

IMPORTANT :

Si la résolution du nom, comme spécifiée ci-dessus, ne fonctionne pas, Data Protector ne peut pas être installé correctement.

Notez également que les noms de l'ordinateur Windows et de l'hôte doivent être identiques. Dans le cas contraire, Data Protector émet un avertissement.

5. Une fois Data Protector installé et une cellule Data Protector créée, vous pouvez utiliser l'outil de vérification DNS pour vérifier que le Gestionnaire de cellule et chaque client sur lequel un Agent de support est installé résolvent correctement les connexions DNS vers tous les autres clients dans la cellule et vice versa. Pour cela, vous devez exécuter la commande `omnicheck -dns` à partir du répertoire `répertoire_Data_Protector\bin`. Les échecs des vérifications, ainsi que leur nombre sont répertoriés.

   Pour obtenir des informations détaillées sur la commande `omnicheck`, reportez-vous au *Guide de référence de l'interface de ligne de commande HP Data Protector*.

Modification du numéro de port par défaut

Modification du numéro de port par défaut de Data Protector

Le service (processus) Data Protector `Inet`, lequel lance les autres processus nécessaires pour la sauvegarde et la restauration, doit utiliser le même nombre de ports sur chaque système de la cellule.

Par défaut, Data Protector utilise le numéro de port 5555. Pour vérifier que ce numéro de port n'est pas utilisé par un autre programme, vous devez afficher `/etc/services` pour les systèmes UNIX ou exécuter la commande `netstat -a`commande sur les systèmes Windows. Si le numéro de port 5555 est déjà utilisé par un autre programme, vous devez modifier cette valeur et la remplacer par un numéro de port encore inutilisé. Si le numéro de port n'est pas disponible sur les systèmes 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. Si les fichiers `/etc/opt/omni/client/customize/socket` et `/opt/omni/newconfig/etc/opt/omni/client/customize/socket` existent sur le système, mettez leur contenu à jour avec le numéro de port requis.

  3. Redémarrez le service `Inet` en terminant le processus concerné à l'aide de la commande `kill -HUP` *`inetd_pid`*. Pour déterminer l'ID de processus (*`inetd_pid`*), tapez la commande `ps -ef`.

  4. Dans le fichier d'options globales, redéfinissez la variable `Port`.

  5. Redémarrez les services Data Protector :

     ```
     /opt/omni/sbin/omnisv stop
     ```

     ```
     /opt/omni/sbin/omnisv start
     ```

Windows

Pour modifier le numéro de port sur un système Windows, procédez comme suit :

- Avant d'installer le Gestionnaire de cellule :

  1. Dans la ligne de commande, exécutez `regedit` pour ouvrir l'Editeur du Registre.

  2. Créez l'entrée de registre `InetPort` sous la clé `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\ OpenView\OmniBackII\Common`.

     Nom de l'entrée de registre : `InetPort`

     Type de l'entrée de registre : `REG_SZ (chaîne)`

     Valeur de l'entrée de registre : *`numéro_port`*

- Une fois le Gestionnaire de cellule installé :

  1. Dans la ligne de commande, exécutez `regedit` pour ouvrir l'Editeur du Registre.

2. Développez **HKEY_LOCAL_MACHINE**, **SOFTWARE**, **Hewlett-Packard**, **OpenView**, **OmniBack** et sélectionnez **Common**.
3. Cliquez deux fois sur **InetPort** pour ouvrir la fenêtre Modification de la chaîne. Dans le champ Données de la valeur, saisissez un numéro de port non utilisé. Procédez de même dans le sous-dossier `Parameters` du dossier `Common`.
4. Dans le panneau de configuration Windows, accédez à Outils d'administration, Services, puis sélectionnez le service **Data Protector Inet** et redémarrez le service (cliquez sur l'icône **Redémarrer** dans la barre d'outils).

Novell NetWare

Pour modifier le numéro de port sur un système Novell NetWare, procédez comme suit :

1. Assurez-vous qu'aucune session Data Protector n'est en cours d'exécution dans la cellule.
2. A partir de la console Novell NetWare, exécutez la commande `UNLOAD HPINET`.
3. Ouvrez le fichier `AUTOEXEC.NCF` et recherchez la ligne suivante :

   ```
   LOAD HPINET.NLM -PORT 5555
   ```

   Remplacez l'entrée `5555` par un numéro de port inutilisé.
4. Ouvrez le fichier `SYS:\ETC\SERVICES` et ajoutez la ligne suivante :

   ```
   omni NuméroPort/tcp
   ```

   `NuméroPort` doit être identique au numéro de port utilisé à l'étape 3 de cette procédure.
5. A partir de la console Novell NetWare, exécutez la commande `WS2_32 RELOAD SERVICES` pour que le système lise à nouveau le fichier `SYS:\ETC\SERVICES`.
6. Exécutez la commande `LOAD HPINET` pour recharger `HPINET`.

Modification du numéro de port par défaut pour l'interface graphique Java

Pour modifier le numéro de port du serveur d'interface Java (555- par défaut), procédez comme suit :

1. Copiez la variable `JGUI_BBC_SERVER_PORT` dans le fichier `omnirc` et attribuez-lui la valeur d'un numéro de port inutilisé.

   Par exemple :

   ```
   JGUI_BBC_SERVER_PORT=5557
   ```

2. Redémarrez les services Data Protector :

   ```
   omnisv -stop
   ```

   ```
   omnisv -start
   ```

Un client d'interface Java doit utiliser le même port pour se connecter au service `UIProxy`.

Lors de la connexion au Gestionnaire de cellule, entrez *`NomGestionnaireCellule:NuméroPort`* dans la boîte de dialogue **Se connecter à un Gestionnaire de cellule** et cliquez sur **Connecter**.

Par exemple :

`mycellmanager:5557`

Préparation d'un cluster de serveur Microsoft sous Windows Server 2008 à l'installation de Data Protector

Pour permettre l'installation du Gestionnaire de cellule Data Protector ou d'un client Data Protector compatible cluster sur un cluster de serveur avec Microsoft Cluster Service (MSCS) exécuté sous le système d'exploitation Windows Server 2008, vous devez préparer le cluster à l'avance. Si vous ignorez cette étape, vous risquez de faire échouer les sessions de sauvegarde de l'objet `CONFIGURATION` local, lequel doit être sauvegardé au cours de la préparation en vue de la reprise après sinistre, et potentiellement de perdre vos données.

Conditions préalables

- Vérifiez que vous êtes connecté au système au moyen d'un compte utilisateur du domaine. Le compte utilisateur du domaine doit être membre du groupe `Administrateurs` local.

Procédure de préparation

Pour préparer correctement votre cluster à l'installation de Data Protector procédez comme suit :

1. Sur les deux noeuds de cluster, démarrez le Pare-feu Windows et autorisez les exceptions pour le programme `Partage de fichiers et d'imprimantes`.
2. Sur le noeud de cluster actif, démarrez la gestion de basculement de cluster et vérifiez que le disque témoin de la ressource quorum est en ligne. Si la ressource est hors ligne, mettez-la en ligne.

   Procédez aux étapes suivantes sur le noeud de cluster actif uniquement.
3. Si vous préparez un cluster sans avoir configuré de Majority Node Set (MNS), démarrez l'Explorateur Windows et transférez la propriété du dossier `LettreDisqueTémoin:\Cluster` au groupe `Administrateurs` local. Lorsque vous modifiez la propriété dans la fenêtre de paramètres de sécurité avancés du cluster, assurez-vous que l'option **Remplacer le propriétaire des sous-conteneurs et des objets** est sélectionnée. Dans la boîte de dialogue Sécurité de Windows, cliquez sur **Oui** pour confirmer la suggestion, puis de nouveau sur **Oui** pour valider la notification qui suit.
4. Si vous préparez un cluster sans avoir configuré de MNS, dans l'Explorateur Windows, modifiez les autorisations sur le dossier `LettreDisqueTémoin:\Cluster` de manière à octroyer le contrôle total au groupe `SYSTEM` et au groupe `Administrateurs` local. Assurez-vous que les paramètres d'autorisation des deux groupes correspondent à ceux présentés dans la Figure 56 à la page 419.

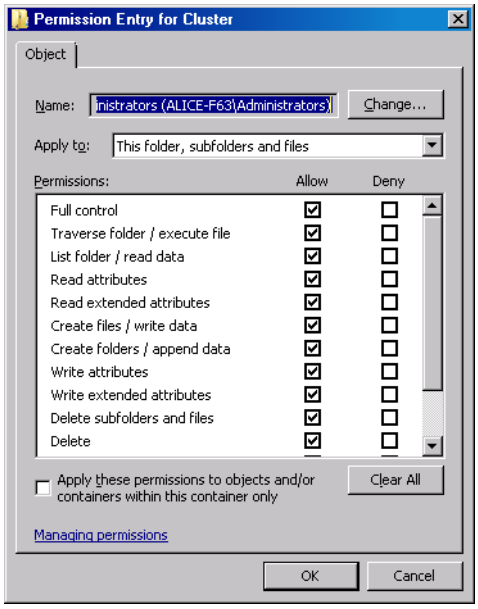


Figure 56 Entrée correcte des autorisations dans le dossier Cluster et le groupe d'utilisateurs local Administrateurs

5. Si vous préparez un cluster qui va assumer le rôle de Gestionnaire de cellule Data Protector, ajoutez une ressource `Point d'accès au cluster` dans le module Gestion du cluster de basculement. Sélectionnez **Ajouter une ressource** et cliquez sur **1- Point d'accès client** pour démarrer l'Assistant Nouvelle ressource :
   a. Dans la fenêtre Point d'accès client, entrez le nom de réseau du serveur virtuel dans la zone de texte Nom.
   b. Entrez l'adresse IP du serveur virtuel dans la zone de texte Adresse.
6. Si vous préparez un cluster qui va assumer le rôle de Gestionnaire de cellule Data Protector, ajoutez un dossier partagé au cluster dans le module Gestion du cluster de basculement. Cliquez sur **Ajouter un dossier partagé** pour démarrer l'assistant Configuration d'un dossier partagé :
   a. Dans la fenêtre Emplacement du dossier partagé, entrez un chemin de répertoire dans la zone de texte Emplacement. Assurez-vous que le répertoire choisi dispose de suffisamment d'espace disque pour stocker les données créées au cours de l'installation de Data Protector. Cliquez sur **Suivant**.
   b. Dans les fenêtres Autorisations NTFS, Protocoles du partage et Paramètres SMB, ne changez pas les valeurs par défaut des options. Cliquez sur **Suivant** pour passer à la fenêtre suivante.

c. Dans le volet Autorisations SMB, sélectionnez l'option **Les administrateurs ont un contrôle total ; tous les autres utilisateurs et groupes ont uniquement un accès en lecture et en écriture**. Cliquez sur **Suivant**.

d. Dans la fenêtre Publication de l'espace de noms DFS, ne modifiez pas les valeurs des options par défaut. Cliquez sur **Suivant**.

e. Dans la fenêtre Revoir les paramètres et créer le partage, cliquez sur **Créer**.

Installation de Data Protector sur Microsoft Cluster Server 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 204.

Une fois que vous avez terminé l'installation, certaines étapes supplémentaires sont requises pour activer le service `Inet Data Protector` permettant de distinguer, entre les ressources disque de cluster et les ressources disque locales, celles qui utilisent leurs propres ressources et non le pilote de ressources Microsoft :

1. Exécutez la commande `omnisv -stop` sur le Gestionnaire de cellule pour arrêter les services et processus Data Protector :

   ```
   répertoire_Data_Protector\bin\omnisv -stop
   ```

2. Définissez une nouvelle variable d'environnement système `OB2CLUSTERDISKTYPES` avec `Volume Manager Disk Group` en tant que valeur ou définissez la variable `omnirc` sur les deux nœuds de cluster comme suit :

   ```
   OB2CLUSTERDISKTYPES=Volume Manager Disk Group
   ```

   Si vous souhaitez spécifier des ressources disque propriétaires supplémentaires, telles qu'un disque NetRAID4, ajoutez simplement le nom du type de la ressource à la valeur de la variable d'environnement `OB2CLUSTERDISKTYPES` :

   ```
   OB2CLUSTERDISKTYPES=Volume Manager Disk Group;NETRaid4M
   Diskset
   ```

   Pour plus d'informations sur l'utilisation des variables de fichier `omnirc`, reportez-vous au *Guide de dépannage HP Data Protector*.

3. Exécutez la commande `omnisv -start` pour démarrer les services/processus :

   ```
   répertoire_Data_Protector\bin\omnisv -start
   ```

Préparation d'un serveur NIS

Cette procédure permet à votre serveur NIS de reconnaître votre Gestionnaire de cellule Data Protector.

Pour ajouter les informations sur Data Protector au serveur NIS, procédez comme suit :

1. Connectez-vous comme utilisateur `root` sur le serveur `NIS`.
2. Si vous gérez le fichier `/etc/services` via `NIS`, ajoutez la ligne suivante au fichier `/etc/services` :

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

   Remplacez 5555 par un autre numéro si ce port n'est pas disponible. Reportez-vous à la section “Modification du numéro de port par défaut de Data Protector” à la page 414.

   Si vous gérez le fichier `/etc/inetd.conf` via `NIS`, ajoutez la ligne suivante au fichier `/etc/inetd.conf` :

   ```
   #Data Protector
   ```

   ```
   omni stream tcp nowait root /opt/omni/lbin/inet -log /var/opt/omni/log/inet.log
   ```
3. Exécutez la commande suivante pour que le serveur `NIS` lise le fichier et mette à jour la configuration.

   ```
   cd /var/yp; make
   ```

REMARQUE :

Dans l'environnement NIS, le fichier `nsswitch.conf` définit l'ordre dans lequel les différents fichiers de configuration seront utilisés. Vous pouvez par exemple définir que le fichier `/etc/inetd.conf` soit utilisé sur la machine locale ou à partir du serveur NIS. Vous pouvez également ajouter une phrase au fichier indiquant que le fichier `nsswitch.conf` contrôle l'emplacement où les noms sont conservés. Pour plus de détails, reportez-vous aux pages du manuel correspondantes.

Si vous avez déjà installé Data Protector, vous devez préparer le serveur NIS, puis redémarrer le service `inet` en arrêtant le processus concerné ; pour cela, utilisez la commande `kill -HUP pid` sur chaque client constituant à la fois un client NIS et un client Data Protector.

Dépannage

- Si le service `Inet Data Protector` ne démarre pas après l'installation de Data Protector dans votre environnement NIS, vérifiez le fichier `/etc/nsswitch.conf`.

  Si vous trouvez la ligne suivante :

  ```
  services: nis [NOTFOUND=RETURN] files
  ```

  remplacez-la par :

  ```
  services: nis [NOTFOUND=CONTINUE] files
  ```

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 228. 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 222.

REMARQUE :

Tous les périphériques et les spécifications de sauvegarde configurés avec l'ancien nom du Gestionnaire de cellule doivent être modifiés en fonction du nouveau nom.

Sous UNIX

Avec un Gestionnaire de cellule UNIX, procédez comme suit :

1. Modifiez les entrées du nom d'hôte du Gestionnaire de cellule dans les fichiers suivants :

   ```
   /etc/opt/omni/client/cell_server
   ```

   ```
   /etc/opt/omni/server/cell/cell_info
   ```

   ```
   /etc/opt/omni/server/users/UserList
   ```

2. Vérifiez que la résolution du nom fonctionne parmi les membres d'une cellule Data Protector.
3. Changez le nom du Gestionnaire de cellule dans la base de données IDB en exécutant la commande suivante :

   ```
   /opt/omni/sbin/omnidbutil -change_cell_name [ancien_hôte]
   ```

Sous Windows

Avec un Gestionnaire de cellule Windows, procédez comme suit :

1. Modifiez les entrées du nom d'hôte du Gestionnaire de cellule dans les fichiers suivants :

   ```
   répertoire_Data_Protector\config\server\cell\cell_info
   répertoire_Data_Protector\config\server\users\userlist
   ```

2. Changez le nom du Gestionnaire de cellule dans la clé de registre suivante :
   `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\ OpenView\ OmniBack\Site\CellServer`

C Tâches associées au périphérique et aux supports

Dans cette annexe

Vous trouverez dans cette annexe des informations supplémentaires relatives aux tâches effectuées dans Data Protector qui dépassent le cadre de ce document, mais qui sont d'importance pour la procédure d'installation. Il s'agit notamment de la configuration du pilote de périphérique, de la gestion des robots SCSI ou encore de la maintenance de l'environnement SCSI.

Utilisation de pilotes de bandes et de pilotes de robots sous Windows

Data Protector prend en charge les pilotes de bandes natifs pour les lecteurs à bandes compatibles rattachés à un système Windows. Les pilotes natifs Windows chargés pour les périphériques changeurs de support (robots) ne sont pas pris en charge par Data Protector.

Dans les exemples ci-dessous, un lecteur de bandes HP 4 mm DDS est relié au système Windows. Vous devez désactiver le pilote natif chargé pour les périphériques changeurs de support si le périphérique à bandes HP 4 mm DDS est connecté à un système Windows et configuré pour être utilisé avec Data Protector. Vous trouverez dans la section ci-dessous la description des procédures correspondantes.

Lecteurs de bandes

Un pilote est généralement fourni avec Windows, si le périphérique est répertorié dans la liste de compatibilité matérielle (HCL). Cette liste regroupe les périphériques supportés par Windows. Vous pouvez la trouver sur Internet, à l'adresse suivante :

http://www.microsoft.com/whdc/hcl/default.mspx

Les pilotes de périphérique sont chargés automatiquement pour tous les périphériques activés une fois que l'ordinateur a été démarré. Il est inutile de charger séparément le pilote de bandes natif, mais vous pouvez le mettre à jour. Pour mettre à jour ou remplacer le pilote de bandes natif sur un système Windows, procédez comme suit :

1. Dans le Panneau de configuration Windows, cliquez deux fois sur **Outils d'administration**.
2. Dans la fenêtre **Outils d'administration**, cliquez deux fois sur **Gestion de l'ordinateur**. Cliquez sur **Gestionnaire de périphériques**.
3. Développez Lecteurs de bande. Pour savoir quel pilote est actuellement chargé pour le périphérique, cliquez avec le bouton droit de la souris sur le lecteur de bandes, puis sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Pilote**, puis sur **Mettre à jour le pilote**. 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.

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 429.

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 :

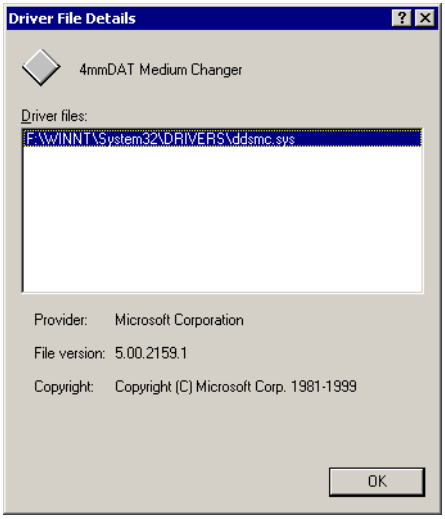


Figure 57 Propriétés du changeur de support

Pour désactiver le pilote de robots natif, cliquez avec le bouton droit de la souris sur **Changeur de support DDS 4mm**, puis sélectionnez **Désactiver**.

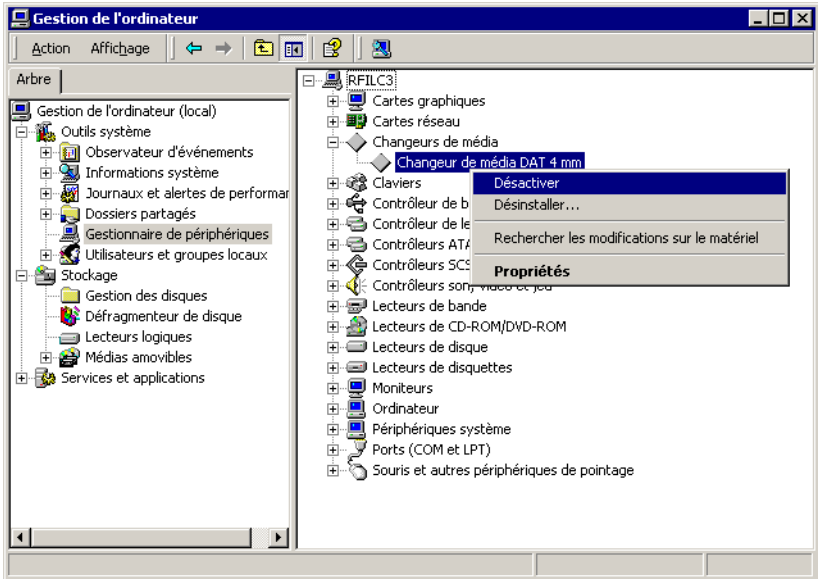


Figure 58 Désactivation des pilotes de robots

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 d'origine

Pour créer un fichier de périphérique pour un lecteur de bande connecté à un système Windows utilisant le pilote de bandes natif, procédez comme suit :

1. Dans le Panneau de configuration Windows, cliquez deux fois sur **Outils d'administration**.
2. Dans la fenêtre Outils d'administration, cliquez deux fois sur **Gestion de l'ordinateur**. Développez Supports amovibles, puis Emplacements physiques. Cliquez avec le bouton droit de la souris sur le lecteur de bandes, puis sélectionnez **Propriétés**.
3. Si le pilote de bandes d'origine est chargé, le nom du fichier du périphérique s'affiche dans la page des propriétés générales. Sinon, vous pouvez trouver les informations utiles dans la page de propriétés Informations sur le périphérique. Reportez-vous à la Figure 59 à la page 430.

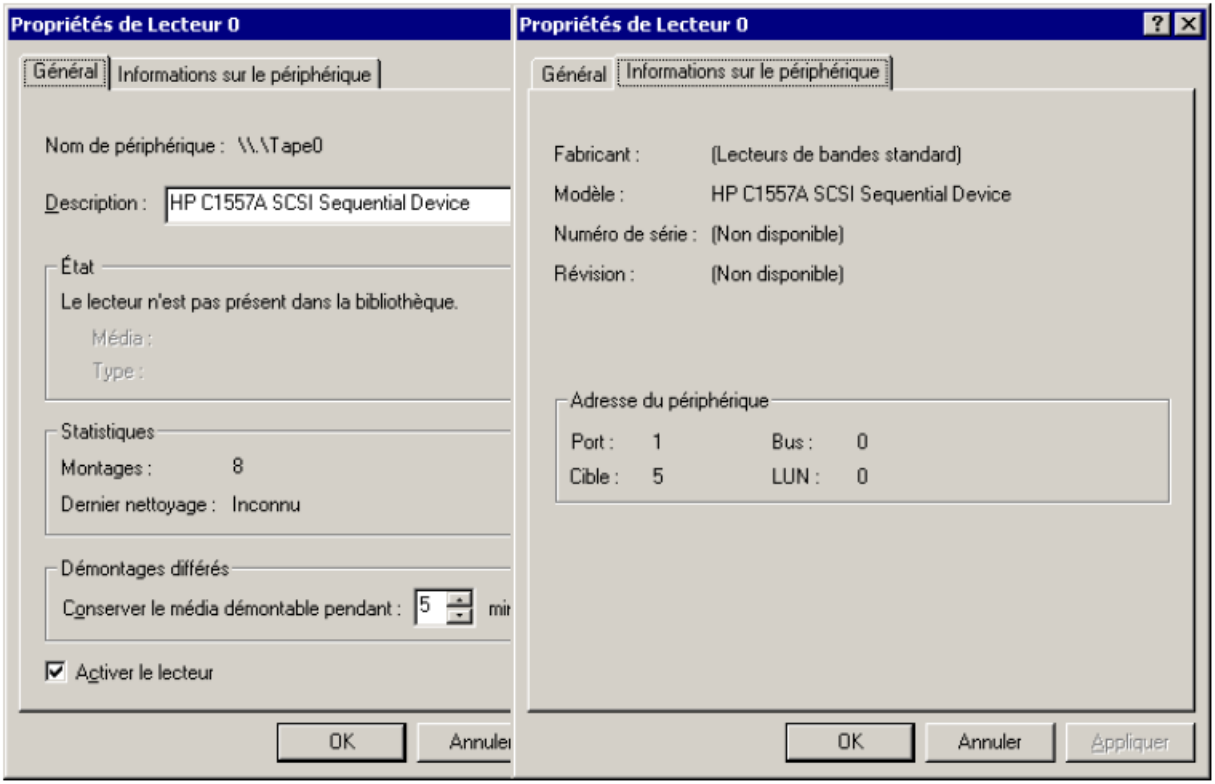


Figure 59 Propriétés du lecteur de bande

Le nom de fichier pour le lecteur de bandes présenté dans la Figure 59 à la page 430 est créé comme suit :

Pilote de bandes natif utilisé	`Tape0` ou `Tape0:0:5:0`
Pilote de bandes natif NON utilisé	`scsi1:0:5:0`

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.

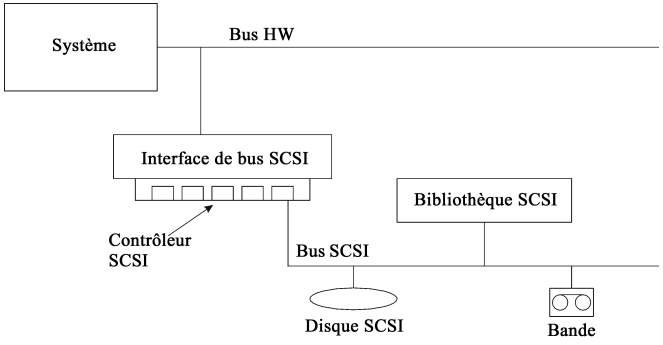


Figure 60 Périphériques SCSI contrôlés

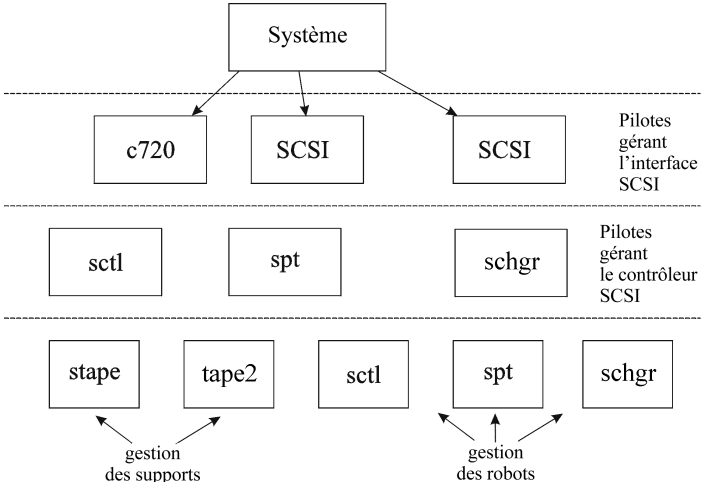


Figure 61 Gestion des périphériques

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 99 du Chapitre 2.

Utilisez la commande `/opt/omni/sbin/ioscan -f` pour savoir si le pilote de robot SCSI est attribué à la bibliothèque que vous souhaitez configurer.

```
root@superhik$ ioscan -f
Class       I  H/W Path    Driver      S/W State H/W Type  Description
=============================================================================
bc          0              root        CLAIMED   BUS_NEXUS
bc          1  8           ccio        CLAIMED   BUS_NEXUS I/O Adapter
unknown    -1  8/0                     CLAIMED   DEVICE    GSC-to-PCI Bus Bridge
ext_bus     0  8/12        c720        CLAIMED   INTERFACE GSC Fast/Wide SCSI Interfac
e
target      0  8/12.0      tgt         CLAIMED   DEVICE
disk        0  8/12.0.0    sdisk       CLAIMED   DEVICE    SEAGATE ST19171W
target      1  8/12.1      tgt         CLAIMED   DEVICE
tape        5  8/12.1.0    stape       CLAIMED   DEVICE    QUANTUM DLT7000
target      2  8/12.2      tgt         CLAIMED   DEVICE
ctl         0  8/12.2.0    sctl        CLAIMED   DEVICE    EXABYTE EXB-210
target      3  8/12.7      tgt         CLAIMED   DEVICE
ctl         0  8/12.7.0    sctl        CLAIMED   DEVICE    Initiator
ba          0  8/16        bus_adapter CLAIMED   BUS_NEXUS Core I/O Adapter
ext_bus     2  8/16/0      CentIf      CLAIMED   INTERFACE Built-in Parallel Interface
audio       0  8/16/1      audio       CLAIMED   INTERFACE Built-in Audio
tty         0  8/16/4      asio0       CLAIMED   INTERFACE Built-in RS-232C
ext_bus     1  8/16/5      c720        CLAIMED   INTERFACE Built-in SCSI
target      4  8/16/5.2    tgt         CLAIMED   DEVICE
disk        2  8/16/5.2.0  sdisk       CLAIMED   DEVICE    TOSHIBA CD-ROM XM-5401TA
target      7  8/16/5.3    tgt         NO_HW     DEVICE
tape        3  8/16/5.3.0  stape       NO_HW     DEVICE    SONY    SDX-300C
target      6  8/16/5.5    tgt         NO_HW     DEVICE
tape        0  8/16/5.5.0  stape       NO_HW     DEVICE    SONY    SDX-300C
target      5  8/16/5.7    tgt         CLAIMED   DEVICE
```

Figure 62 Etat du pilote de passage SCSI (sctl)

La Figure 62 à la page 432 vous indique le pilote de passage SCSI `sctl` affecté au périphérique de contrôle du périphérique à bandes Exabyte. Le chemin matériel correspondant (H/W Path) est `8/12.2.0`. (SCSI=2, LUN=0).

Un lecteur de bandes est connecté au même bus SCSI, mais le pilote qui le contrôle est `stape`. Le chemin de matériel correspondant (H/W Path) est `8/12.1.0`. (SCSI=0, LUN=0)

IMPORTANT :

L'adresse SCSI 7 est toujours utilisée par les contrôleurs SCSI, bien que la ligne correspondante n'apparaisse pas forcément dans les résultats de la commande `ioscan -f`. Dans cet exemple, le contrôleur est géré par `sctl`.

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
=============================================================
bc          0            root      CLAIMED   BUS_NEXUS
ext_bus     0  52        scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1      target    CLAIMED   DEVICE
disk        4  52.1.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2      target    CLAIMED   DEVICE
disk        0  52.2.0    disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4      target    CLAIMED   DEVICE
tape        0  52.4.0    tape2     CLAIMED   DEVICE    HP       C1533A
spt         1  52.4.1    spt       CLAIMED   DEVICE    HP       C1553A
target      6  52.5      target    CLAIMED   DEVICE
disk        5  52.5.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6      target    CLAIMED   DEVICE
disk        1  52.6.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56        lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0      mux4      CLAIMED   INTERFACE
lan         0  56.1      lan3      CLAIMED   INTERFACE
lantty      0  56.2      lantty0   CLAIMED   INTERFACE
processor   0  62        processor CLAIMED   PROCESSOR Processor
memory      0  63        memory    CLAIMED   MEMORY    Memory
# 
```

Figure 63 Etat du pilote de passage SCSI - spt

La Figure 63 à la page 433 donne un exemple de périphérique à bandes connecté, avec un robot contrôlé par le pilote de passage SCSI `spt`. Le périphérique en question est un périphérique de bibliothèque de bandes HP StorageWorks 12000e qui utilise l'adresse SCSI 4 et est connecté au bus SCSI avec le chemin matériel 52. Le chemin matériel correspondant est 52.4.1. Le robot est correctement affecté au pilote de passage SCSI `spt`.

Si le pilote `sctl`, `spt` ou `schgr` n'est pas affecté au robot, vous devez ajouter le chemin matériel du robot à l'instruction du pilote dans le fichier `system`, puis recréer le noyau. Pour cela, suivez la procédure ci-dessous.

Pour ajouter *manuellement* un pilote de robot SCSI au noyau, l'affecter au robot, puis recréer manuellement un nouveau noyau, procédez comme suit :

1. Connectez-vous comme utilisateur *root*, puis basculez vers le répertoire build :

   ```
   cd /stand/build
   ```

2. Créez un fichier système à partir du noyau existant :

   ```
   /usr/lbin/sysadm/system_prep -s system
   ```

3. Vérifiez quel pilote de robot SCSI est déjà intégré au kernel en cours. A partir du répertoire `/stand`, tapez la commande suivante :

   grep *`pilote de robot SCSI`***system**

   où `pilote de robot SCSI` peut être `spt`, `sctl` ou `schgr`. Le système affiche alors la ligne correspondante si le pilote est déjà intégré au noyau en cours.

4. Utilisez un éditeur pour ajouter une instruction de pilote :

   ```
   driver chemin matériel spt
   ```

   au fichier `/stand/build/system`, où `chemin matériel` correspond au chemin matériel complet du périphérique.

   Pour la bibliothèque de bandes HP StorageWorks 12000e de l'exemple précédent, vous auriez saisi :

   ```
   driver 52.4.1 spt
   ```

   Si plusieurs bibliothèques sont connectées au même système, vous devez ajouter une ligne de pilote pour chaque robot de bibliothèque, avec le chemin matériel approprié.

   Lorsque vous configurez le pilote `schgr`, ajoutez la ligne suivante à l'instruction de pilote :

   ```
   schgr
   ```

5. Tapez la commande `mk_kernel -s./system` pour construire un nouveau noyau.

6. Enregistrez l'ancien fichier system sous un autre nom et renommez le nouveau fichier system avec le nom initial pour qu'il devienne le fichier en vigueur :

   ```
   mv /stand/system /stand/system.prev
   ```

   ```
   mv /stand/build/system /stand/system
   ```

7. Enregistrez l'ancien kernel sous un autre nom et renommez le nouveau kernel avec le nom initial pour qu'il deviennent le 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 le réamorçage du système, vérifiez vos modifications à l'aide de la commande **/usr/sbin/ioscan -f**.

Création de fichiers de périphérique sous HP-UX

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. 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 63 à la page 433 vous présente les résultats de la commande `ioscan -f` sur le système HP-UX sélectionné.

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
=============================================================
bc          0           root      CLAIMED   BUS_NEXUS
ext_bus     0  52       scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1     target    CLAIMED   DEVICE
disk        4  52.1.0   disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2     target    CLAIMED   DEVICE
disk        0  52.2.0   disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4     target    CLAIMED   DEVICE
tape        0  52.4.0   tape2     CLAIMED   DEVICE    HP       C1533A
spt         1  52.4.1   spt       CLAIMED   DEVICE    HP       C1553A
target      6  52.5     target    CLAIMED   DEVICE
disk        5  52.5.0   disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6     target    CLAIMED   DEVICE
disk        1  52.6.0   disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56       lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0     mux4      CLAIMED   INTERFACE
lan         0  56.1     lan3      CLAIMED   INTERFACE
lantty      0  56.2     lantty0   CLAIMED   INTERFACE
processor   0  62       processor CLAIMED   PROCESSOR Processor
memory      0  63       memory    CLAIMED   MEMORY    Memory
# 
```

Figure 64 Liste des périphériques connectés

L'interface du bus SCSI est contrôlée par le pilote système `scsi1`. Il s'agit d'une interface `SCSI NIO`. Pour accéder au robot de bibliothèque sur le bus `SCSI NIO`, il faut utiliser le pilote de passage SCSI `spt` qui est déjà installé et affecté au robot

du périphérique à bandes HP StorageWorks 12000e, lequel utilise le chemin matériel `52.4.1`.

REMARQUE :

Si vous n'utilisez pas une interface de bus basée sur `SCSI NIO`, le pilote `spt` n'est pas nécessaire, mais le pilote `sctl` est utilisé à sa place.

Pour créer un fichier de périphérique, vous devez connaître le *numéro majeur* du pilote de passage SCSI et le *numéro mineur*, qui ne dépend pas du pilote de passage SCSI que vous utilisez.

Pour obtenir le *numéro majeur* correspondant au `spt`, exécutez la commande suivante :

```
lsdev -d spt
```

Dans notre exemple (voir la Figure 64 à la page 435), 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` -> Le *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 utilisateur graphique 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 65 à la page 438 présente les résultats de la commande `/usr/sbin/ioscan -f` sur un système HP-UX 11.x.

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
=============================================================================
bc          0             root      CLAIMED   BUS_NEXUS
ext_bus     0  52         scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1       target    CLAIMED   DEVICE
disk        4  52.1.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2       target    CLAIMED   DEVICE
disk        0  52.2.0     disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4       target    CLAIMED   DEVICE
tape        0  52.4.0     tape2     CLAIMED   DEVICE    HP       C1533A
spt         1  52.4.1     spt       CLAIMED   DEVICE    HP       C1553A
target      6  52.5       target    CLAIMED   DEVICE
disk        5  52.5.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6       target    CLAIMED   DEVICE
disk        1  52.6.0     disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56         lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0       mux4      CLAIMED   INTERFACE
lan         0  56.1       lan3      CLAIMED   INTERFACE
lantty      0  56.2       lantty0   CLAIMED   INTERFACE
processor   0  62         processor CLAIMED   PROCESSOR Processor
memory      0  63         memory    CLAIMED   MEMORY    Memory
#
```

Figure 65 Résultats de ioscan -f sur un système HP-UX :

Seules la troisième (`chemin H/W`) et la cinquième (`état S/W`) colonnes sont utiles pour déterminer les adresses SCSI disponibles. Un format de (`chemin H/W`) démembré se présenterait sous la forme suivante :

`Chemin_H/W_bus_SCSI.adresse_SCSI.numéro_LUN`

Dans ce cas particulier, il n'y a qu'un bus SCSI, qui utilise le chemin H/W 52. Pour ce bus, vous pouvez utiliser les adresses SCSI `0` et 3, puisqu'elles ne figurent pas dans la liste.

La Figure 65 à la page 438 vous indique quelles sont les adresses du bus SCSI sélectionné qui sont déjà occupées :

- L'adresse SCSI 1 est occupée par un disque SCSI.
- L'adresse SCSI 2 est occupée par un CD-ROM.
- L'adresse SCSI 4, LUN 0, est occupée par un lecteur de bandes.
- L'adresse SCSI 4, LUN 1, est occupée par la bibliothèque de bandes.
- L'adresse SCSI 5 est occupée par un disque SCSI.
- L'adresse SCSI 6 est occupée par un disque SCSI.
- L'adresse SCSI 7 est occupée par un contrôleur SCSI.

REMARQUE :

Bien que l'adresse SCSI numéro 7 *ne* figure *pas* dans la liste, elle est occupée par défaut par le contrôleur SCSI.

Pour tous les périphériques, la valeur `Etat S/W` est définie à `UTILISE` (CLAIMED) et la valeur `Type H/W` est définie à `PERIPHERIQUE` (H/W DEVICE) ce qui signifie que les périphériques sont actuellement connectés. Si une valeur `INUTILISE` (UNCLAIMED) figurait dans la colonne `Etat S/W` ou `AUCUN PERIPHERIQUE` (NO H/W) dans la colonne `Type H/W`, cela signifierait que le système ne peut pas accéder au périphérique.

L'adresse SCSI 4 est demandée par la bibliothèque de bandes, dotée du lecteur de bandes avec le LUN 0 et du robot avec le LUN 1. Le lecteur est contrôlé par le pilote `tape2` et le robot par le pilote de passage SCSI `spt`. Dans la description, vous pouvez constater que le périphérique est une bibliothèque HP StorageWorks 12000e ; celle-ci est facilement reconnaissable parmi les autres bibliothèques SCSI car elle utilise la même adresse SCSI pour le lecteur de bandes et le robot, mais avec des LUN différents.

Tout le bus SCSI est contrôlé par le module d'interface `scsi1`.

Recherche des ID SCSI cibles inutilisés sous Solaris

L'accès et le contrôle d'un périphérique de sauvegarde connecté à un système Solaris se fait via un fichier de périphérique. Ce fichier de périphérique est automatiquement

créé par le système d'exploitation Solaris dans le répertoire `/dev/rmt`, au moment de la connexion du périphérique de sauvegarde et de la mise sous tension du système client et du périphérique de sauvegarde.

Toutefois, avant de connecter le périphérique de sauvegarde, les adresses SCSI disponibles doivent être vérifiées et l'adresse du périphérique de sauvegarde doit être établie sur une adresse non encore allouée.

Pour répertorier les adresses SCSI disponibles sur un système Solaris, procédez comme suit :

1. Arrêtez le système en appuyant sur **Stop** et **A**.
2. A l'invite ok, exécutez la commande **probe-scsi-all** :

   probe-scsi-all

   Le système peut vous demander de lancer la commande `reset-all` avant d'exécuter la commande `probe-scsi-all`.
3. Pour revenir au fonctionnement normal, tapez **go** à l'invite `ok` :

   `go`

Après avoir répertorié les adresses disponibles et choisi celle que vous souhaitez utiliser pour votre périphérique de sauvegarde, vous devez mettre à jour les fichiers de configuration appropriés avant de connecter et de démarrer le périphérique. Reportez-vous à la section suivante pour obtenir des instructions sur la mise à jour des fichiers de configuration.

Mise à jour de la configuration des périphériques et pilotes sur un système Solaris

Mise à jour des fichiers de configuration

Les fichiers de configuration suivants servent à la configuration du périphérique et du lecteur. Ils doivent être vérifiés, et modifiés le cas échéant, avant que les périphériques connectés ne puissent être utilisés :

- `st.conf`
- `sst.conf`

st.conf : Tous les périphériques

Ce fichier est requis sur tout client Solaris Data Protector auquel est connecté un périphérique à bandes. Il doit contenir des informations sur le périphérique et une ou plusieurs adresses SCSI pour chaque périphérique de sauvegarde connecté au client. Une seule entrée SCSI est requise pour un périphérique à lecteur unique, tandis qu'il en faut plusieurs pour un périphérique de bibliothèque multi-lecteurs.

1. Vérifiez quelles sont les adresses SCSI inutilisées sur le client, tel que le décrit la section précédente, et choisissez une adresse pour le périphérique à connecter.
2. Définissez les adresses SCSI choisies sur le périphérique de sauvegarde.
3. Eteignez le système client.
4. Connectez le périphérique de sauvegarde.
5. Remettez le périphérique sous tension, puis le système client.
6. Arrêtez le système en appuyant sur `Stop` et `A`.
7. A l'invite `ok`, tapez la commande **probe-scsi-all** :

   ```
   probe-scsi-all
   ```

   Cela permet de fournir des informations sur les périphériques SCSI connectés, notamment la chaîne d'identification correcte du périphérique de sauvegarde nouvellement connecté.
8. Revenez en fonctionnement normal :

   ```
   go
   ```

9. Modifiez le fichier `/kernel/drv/st.conf`. Ce fichier est utilisé par le pilote (bande SCSI) `st` de Solaris. Il contient une liste des périphériques officiellement pris en charge par Solaris, ainsi qu'un ensemble de saisies de configuration pour des périphériques tiers. Si vous utilisez un périphérique non pris en charge, il devrait être possible de le connecter et de l'utiliser sans configuration supplémentaire. Sinon, vous pouvez ajouter les types d'entrée suivants dans le fichier `st.conf` :

   - Une entrée de liste de configuration de bande (plus une définition de variable de données de bandes). Des exemples d'entrées, accompagnés de commentaires, sont fournis dans le fichier. Si l'un d'eux vous convient, vous pouvez l'utiliser ; vous pouvez également les modifier pour les adapter à vos besoins.

     L'entrée doit venir avant la première entrée `name=` du fichier et le format requis est le suivant :

     tape-config-list= "`périphérique à bandes`", "`nom de référence du périphérique à bandes`", "`données de bandes`";

     où :

`périphérique à bande`	Chaîne d'identification du fournisseur et du produit pour le périphérique à bandes. Celui-ci doit être correctement spécifié, en conformité avec la documentation du constructeur du périphérique.
`nom de référence du périphérique à bandes`	Nom que vous choisissez, par lequel le système identifiera le périphérique à bandes. Ce nom ne modifie pas l'identification du produit mais, lorsque le système démarre, c'est le nom de référence qui s'affiche la liste des périphériques reconnus par le système.
`données de bandes`	Variable qui fait référence à des éléments supplémentaires de configuration du périphérique à bandes. La définition de la variable doit elle aussi être indiquée correctement,

conformément aux dispositions de la documentation du constructeur du périphérique.

comme l'illustre l'exemple suivant :

```
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.

  comme l'illustre l'exemple suivant :

  ```
  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.

  comme l'illustre l'exemple suivant :

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

sst.conf : périphériques de bibliothèque

Ce fichier requis sur chaque client Solaris Data Protector auquel un périphérique de bibliothèque multi-lecteurs est connecté. D'une manière générale, il requiert une entrée pour l'adresse SCSI du mécanisme de robot de chacun des périphériques de bibliothèque connectés au client. Il existe cependant quelques exceptions, à l'instar du HP StorageWorks 24x6 mentionné dans la section précédente.

1. Copiez le pilote (module) `sst` et le fichier de configuration `sst.conf` dans le répertoire requis :
   - Pour les systèmes d'exploitation 32 bits :
     ```
     $cp /opt/omni/spt/sst /usr/kernel/drv/sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```
   - Pour les systèmes d'exploitation 64 bits :
     ```
     $cp /opt/omni/spt/sst.64bit /usr/kernel/drv/sparcv9 /
     sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```
2. Modifiez le fichier `sst.conf` et ajoutez l'entrée suivante :

   name="sst" class="scsi" target=*X* **lun=***Y***;**

   où :

   X correspond à l'adresse SCSI du mécanisme du robot.

   Y est l'unité logique.

   comme l'illustre l'exemple suivant :

   ```
   name="sst" class="scsi" target=6 lun=0;
   ```
3. Ajoutez le pilote au noyau Solaris :

   ```
   add_drv sst
   ```

Création et vérification de fichiers de périphérique

Après avoir défini les fichiers de configuration et installé les pilotes, vous pouvez créer de nouveaux fichiers de périphérique comme suit :

1. Supprimez tous les fichiers de périphérique existants du répertoire `/dev/rmt` :

   ```
   cd /dev/rmt rm *
   ```
2. Tapez la commande suivante pour arrêter le système :

   ```
   shutdown -i0 -g0
   ```

3. Relancez le système :

   ```
   boot -rv
   ```

   Le commutateur `r` de la commande `boot` permet une compilation du noyau et inclut la création de fichiers de périphérique spéciaux utilisés pour la communication avec le périphérique à bandes. Le commutateur `v` active l'affichage en mode prolixe (verbose) du démarrage du système. Avec le mode prolixe, le système indique que le périphérique est connecté en affichant la chaîne *`nom de référence du périphérique à bandes`* que vous avez sélectionnée lors de la phase de l'initialisation relative à la configuration du répertoire `/devices`.

4. Tapez la commande suivante pour vérifier l'installation :

   ```
   mt -t /dev/rmt/0 status
   ```

   La sortie de cette commande dépend du lecteur configuré. Elle se présente de la manière suivante :

   ```
   Quantum DLT7000 tape drive: sense key(0x6)= Unit Attention
   residual= 0 retries= 0 file no= 0 block no= 0
   ```

5. Une fois que la réinitialisation est terminée, vous pouvez vérifier les fichiers de périphérique qui ont été créés à l'aide de la commande `ls -all.` Pour un périphérique de bibliothèque, le résultat de cette commande peut être le suivant :

/dev/rmt/0hb	pour un premier lecteur de bandes
/dev/rmt/1hb	pour un deuxième lecteur de bandes
/dev/rsst6	pour un lecteur de robot

Recherche des ID SCSI cibles inutilisés sur un système Windows

Pour déterminer quels sont les ID SCSI cibles (adresses SCSI) inutilisés sur un système Windows, procédez comme suit :

1. Dans le Panneau de configuration Windows, cliquez deux fois sur **Adaptateurs SCSI**.

2. Vérifiez les propriétés de chaque périphérique connecté à une carte SCSI de la liste. Cliquez deux fois sur le nom d'un périphérique, puis sélectionnez **Paramètres** pour ouvrir sa page de propriétés. Reportez-vous à la Figure 66 à la page 447.

   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.

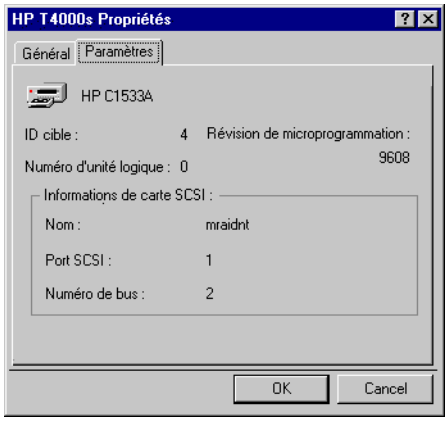


Figure 66 Paramètres du périphérique

Configuration des ID SCSI sur une bibliothèque HP StorageWorks 330fx

Une fois que vous avez choisi les ID SCSI pour le robot et les lecteurs, vous pouvez les vérifier et les configurer à l'aide du panneau de configuration de la bibliothèque.

EXEMPLE : si vous disposez d'une bibliothèque HP StorageWorks 330fx, procédez comme suit pour trouver les ID SCSI configurés :

1. Depuis l'état PRET, appuyez sur **SUIVANT**. `ADMIN*` apparaît.
2. Appuyez sur **ENTREE**. Vous êtes invité à saisir le mot de passe. Saisissez le mot de passe.
3. `TEST*` apparaît ; appuyez sur **SUIVANT** jusqu'à ce que l'option `ID SCSI*` apparaisse.
4. Appuyez sur **ENTREE**. `VIEW IDs*` apparaît.
5. Appuyez sur **ENTREE**. `JKBX ID 6 LUN 0` s'affiche.

6. Appuyez sur **SUIVANT**. `DRV 1 ID 5 LUN 0` s'affiche.
7. Appuyez sur **SUIVANT**. `DRV 2 ID 4 LUN 0` s'affiche, etc.

Vous pouvez revenir à l'état PRET en appuyant sur ANNULER plusieurs fois.

Connexion de périphériques de sauvegarde

Pour connecter un périphérique de sauvegarde à un système HP-UX, Solaris, Linux ou Windows, suivez la procédure générale ci-dessous.

1. Sélectionnez le client auquel vous souhaitez connecter le périphérique de sauvegarde.
2. Installez un Agent de support sur le système sélectionné. Reportez-vous à la section “Installation distante de clients Data Protector” à la page 83.

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 438. Pour les systèmes Solaris, reportez-vous à la section "Recherche des ID SCSI cibles inutilisés sous Solaris" à la page 439. Pour les systèmes Windows, reportez-vous à la section "Recherche des ID SCSI cibles inutilisés sur un système Windows" à la page 446.

   - Pour la connexion à un système HP-UX, vérifiez que les pilotes requis sont *installés* et *intégrés* au noyau en cours. Reportez-vous à la section "Vérification de la configuration du noyau sous HP-UX" à la page 100.

     Si vous devez configurer un pilote de passage SCSI, reportez-vous à la section "Configuration de robot SCSI sous HP-UX" à la page 431.
   - 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 440. 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 425.

     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 429.

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 447.

   Pour obtenir des informations détaillées sur les périphériques pris en charge, consultez le site 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 435.

   - Sur un système Solaris, exécutez l'utilitaire `ls -all` dans le répertoire `/dev/rmt` pour afficher la liste des périphériques connectés, avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver le nouveau périphérique connecté avec les adresses SCSI correctes.
   - Sur un système Solaris, exécutez l'utilitaire `ls -all` dans le répertoire `/dev/rmt` pour afficher la liste des périphériques connectés, avec les chemins matériels et les fichiers de périphérique correspondants, dans laquelle vous devez trouver le nouveau périphérique connecté avec les adresses SCSI correctes.
   - Sur un système Windows, vous pouvez vérifier que le système reconnaît correctement le nouveau périphérique de sauvegarde à l'aide de l'utilitaire `devbra`. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez :

     `devbra -dev`

     Dans les résultats de la commande `devbra`, vous trouverez pour chaque périphérique connecté et correctement reconnu les lignes suivantes :

     `spécification du périphérique de sauvegarde`

     `chemin_matériel`

     `type_support`

     `.....`

     Par exemple, les résultats suivants :

     `HP:C1533A`

     `tape3:0:4:0`

     `DDS`

```
...
...
```

signifient qu'un périphérique à bandes HP DDS (le pilote de bandes natif étant chargé) a le numéro d'instance du lecteur 3, et est connecté au bus SCSI 0, à l'ID SCSI cible 4 et au numéro LUN 0.

Tandis que les résultats suivants :

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

signifient qu'un périphérique à bandes HP DDS (le pilote de bandes d'origine étant déchargé) est connecté au port SCSI 1, au bus SCSI 0 et que le lecteur de bandes a l'ID SCSI cible 4 et le numéro LUN 0.

- Sur un système AIX, servez-vous de l'utilitaire `lsdev`

  ```
  lsdev -C
  ```

  pour afficher la liste des périphériques connectés et les noms de périphérique correspondants.

Compression matérielle

La plupart des périphériques de sauvegarde récents proposent une compression matérielle intégrée pouvant être activée lors de la création d'un fichier de périphérique ou d'une adresse SCSI pendant la procédure de configuration du périphérique. Reportez-vous à l'aide en ligne pour connaître la procédure détaillée.

La compression matérielle est effectuée par un périphérique qui reçoit les données originales d'un Agent de support et les écrit sur la bande sous forme compressée. Ce procédé permet d'augmenter la vitesse à laquelle un lecteur de bande reçoit les données car le volume de données écrit sur la bande est moins important.

Lorsque la compression logicielle est utilisée et la compression matérielle désactivée, les données sont compressées par l'Agent de disque et envoyées sous forme compressée à un Agent de support. L'algorithme de compression peut faire appel à une quantité de ressources de l'Agent de disque considérable si la compression logicielle est utilisée, mais cela réduit la charge réseau.

Pour activer la compression matérielle sous Windows, ajoutez “C” à la fin des adresses SCSI de périphérique/lecteur, par exemple : scsi:0:3:0C (ou tape2:0:1:0C si le pilote du lecteur de bandes est chargé). Si le périphérique prend en charge la compression matérielle, celle-ci sera utilisée ; sinon, l'option C sera ignorée.

Pour désactiver la compression matérielle sous Windows, ajoutez “N” à la fin de l'adresse SCSI du 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 83.

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 100.
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 438.
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 446.
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 100.
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 431.
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 438.

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 435.

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 446.
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 100.
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 431.

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 438.

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 435.
8. Vérifiez que le système reconnaît correctement le nouveau fichier de périphérique du robot de bibliothèque. Servez-vous de l'utilitaire `ioscan` :

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

   Le nouveau fichier de périphérique doit apparaître dans les résultats de la commande.

Etape suivante

Une fois le périphérique de la bibliothèque DLT 28/48 logements HP StorageWorks correctement connecté, recherchez : "configuration, périphériques de sauvegarde" dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

Connexion à un système Solaris

Pour configurer le périphérique de bibliothèque HP C5173-7000 sur un système Solaris, exécutez la procédure décrite ci-dessous. Cet exemple suppose que deux lecteurs sont alloués à Data Protector :

1. Copiez le pilote (module) `sst` et le fichier de configuration `sst.conf` dans le répertoire requis :
   - Pour les systèmes d'exploitation 32 bits :
     ```
     $cp /opt/omni/spt/sst /usr/kernel/drv/sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv/sst.conf
     ```
   - Pour les systèmes d'exploitation 64 bits :
     ```
     $cp /opt/omni/spt/sst.64 /usr/kernel/drv/sparcv9 /sst
     $cp /opt/omni/spt/sst.conf /usr/kernel/drv /sparcv9/
     sst.conf
     ```
2. Ajoutez le pilote au noyau Solaris :
   ```
   add_drv sst
   ```
3. Supprimez tous les fichiers de périphérique existants du répertoire `/dev/rmt` :
   ```
   cd /dev/rmt rm *
   ```
4. Arrêtez le système en appuyant sur **Stop** et `A.`
5. Exécutez la commande `probe-scsi-all` à l'invite "`ok`" pour vérifier quelles sont les adresses SCSI disponibles.
   ```
   ok probe-scsi-all
   ```
   Le système peut vous demander de lancer la commande `reset-all` avant d'exécuter la commande `probe-scsi-all`.

   Dans le cas présent, nous utiliserons le port 6 pour le périphérique de contrôle SCSI, le port 2 pour le premier lecteur et le port 1 pour le deuxième lecteur ; le numéro LUN est 0.
6. Revenez en fonctionnement normal :
   ```
   ok go
   ```
7. Copiez le fichier de configuration `st.conf` dans le répertoire requis :
   ```
   $cp /opt/omni/spt/st.conf /kernel/drv/st.conf
   ```
   Le fichier `st.conf` est présent sur chaque client Data Protector Solaris et contient les adresses SCSI de chaque périphérique de sauvegarde connecté au client.

8. Modifiez le fichier `/kernel/drv/st.conf` et ajoutez les lignes suivantes :

```
tape-config-list= "QUANTUM DLT7000", "Digital DLT7000",
"DLT-data3";

DLT-data3 = 1,0x77,0,0x8639,4,0x82,0x83,0x84,0x85,3;

name="st" class="scsi"

target=1 lun=0;

name="st" class="scsi"

target=2 lun=0;

name="st" class="scsi"

target=6 lun=0;
```

   Ces entrées fournissent les adresses SCSI pour le lecteur 1, le lecteur 2 et le robot.

9. Modifiez le fichier `sst.conf` (que vous avez copié à l'Étape 1 à la page 459) et ajoutez la ligne suivante :

```
name="sst" class="scsi" target=6 lun=0;
```

REMARQUE :

Cette entrée doit être identique à celle du robot dans le fichier `st.conf`. Reportez-vous à l'Étape 8 à la page 460 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 446.
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 446.
2. Définissez les adresses SCSI (ID cibles) sur le périphérique. Pour obtenir des informations détaillées, consultez la documentation fournie avec le périphérique.

1. Allumez d'abord le périphérique, puis l'ordinateur, et attendez que le processus d'amorçage soit terminé.
2. Vérifiez que le système reconnaît correctement les nouveaux lecteurs de bandes connectés et le robot. Dans le répertoire `répertoire_Data_Protector\bin`, exécutez :

   ```
   devbra -dev
   ```

   Dans les résultats de la commande `devbra`, vous devez trouver le nouveau lecteur de bandes connecté du lecteur de bandes Seagate Viper 200 LTO Ultrium.

Etape suivante

Une fois le lecteur de bandes Seagate Viper 200 LTO Ultrium correctement connecté, recherchez : "configuration, périphériques de sauvegarde" dans l'index de l'aide en ligne pour obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour le périphérique que vous venez de connecter.

REMARQUE :

Lorsque vous configurez le lecteur de bandes Seagate Viper 200 LTO Ultrium avec Data Protector, assurez-vous que le mode de compression est activé. Pour cela, spécifiez le paramètre `C` après l'adresse SCSI du lecteur, par exemple :

```
scsi2:0:0:0C
```

Vérification de l'installation de l'Agent général de support sous Novell NetWare

Après avoir effectué l'installation de l'Agent général de support sur la plateforme Novell NetWare, vous devez la contrôler en procédant comme suit :

- Identifiez le périphérique de stockage.
- Testez le démarrage de l'Agent général de support sur la console du serveur Novell NetWare.
- Testez le démarrage de `HPUMA.NLM` et de `HPDEVBRA.NLM` sur la console du serveur Novell NetWare.

Identification du périphérique de stockage

Utilisez la convention suivante pour identifier un périphérique de stockage dans l'environnement Novell NetWare :

`numéro d'identification de la carte``:`*`numéro d'identification cible`*`:`*`numéro d'unité logiquecompression`*

Par exemple, la chaîne “`0:2:0N`” identifie un périphérique de stockage avec comme ID de carte 0, comme ID cible 2, un numéro d'unité logique (LUN) 0 et aucune compression.

Autre exemple : la chaîne “`1:1:0C`” identifie un périphérique de stockage avec comme ID de carte 1, comme ID cible 1, un numéro d'unité logique (LUN) 0 et la compression activée.

Test de démarrage de l'Agent général de support

Une fois l'Agent général de support installé sur le système Novell NetWare, vous pouvez tester le démarrage d'un Agent de support de sauvegarde `HPBMA.NLM` sur la console du serveur Novell NetWare.

Dans l'exemple ci-après, la carte bus hôte `Adaptec`, `AHA-2940`, est utilisée pour accéder au périphérique à bandes échangeur de la bibliothèque de bandes HP StorageWorks 12000e.

Avant de démarrer tout composant `*.NLM` de Data Protector, vous devez satisfaire aux conditions suivantes :

- `HPINET` doit être en cours d'exécution.
- Le pilote de carte hôte SCSI `Adaptec` doit être en cours d'exécution.
- Le logiciel de l'Agent général de support doit se trouver dans le répertoire `SYS:USR\OMNI\BIN`.
- Le périphérique de stockage doit être correctement installé et connecté.
- La carte bus hôte Adaptec et le protocole de communication TCP/IP doivent être correctement installés et en cours d'exécution.

Une fois ces conditions remplies, procédez comme suit :

1. Pour charger `HPBMA.NLM`, tapez :

   `LOAD HPBMA -name testbma -type` *`numéro_type`* `-policy` *`numéro_mode`* `-ioctl périphérique_contrôle -dev périphérique_données -tty` *`numéro_port_TCP`*

   L'option `type` *`numéro_type`* correspond au type de périphérique Data Protector. Les valeurs possibles pour *`numéro_type`* sont les suivantes :

   - 1=DAT/DDS
   - 2 = QIC (cartouche d'un quart de pouce)
   - 3 = Exabyte 8mm
   - 9 = périphérique générique à bandes magnétiques
   - 10 = bande linéaire numérique (DLT)

   L'option `policy` *`numéro_mode`* correspond au mode d'utilisation du périphérique par Data Protector. Les valeurs possibles sont les suivantes :

   - 1= périphérique autonome
   - 10= bibliothèque SCSI - II

   L'option `ioctl` *`périphérique_contrôle`* définit l'adresse SCSI du contrôle du robot. Elle se présente sous la forme suivante :

   `numéro_identification_adaptateur`:*`numéro_identification_cible`*:

   `numéro_unité_logique`

   comme l'illustre l'exemple suivant :

   - `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`

   comme l'illustre l'exemple suivant :

   - `0:1:1C` =>Le périphérique de contrôle (robot) utilise la carte SCSI 0, possède l'adresse SCSI 1 et le LUN 1. La compression de données est activée.

   L'option `-tty` *`numéro_port_TCP`* correspond au numéro de port du protocole de communication TCP/IP.

L'Agent de support de la console, HPCONMA.NLM, démarre et l'écran suivant s'affiche :

```
*** MA listening on port: numéro

SLOT: [Load(2), Peek(2), Stop(0), Abort(0)]

SLOT: _
```

Les commandes actuellement disponibles sont les suivantes :

`Load(2)` - Cette commande permet de charger la bande dans le lecteur et requiert deux arguments :

`Load` *`numéro d'emplacementindicateur de permutation`*

L'indicateur de permutation peut être défini soit à 0 soit à 1, ce qui signifie que le support ne permute pas si la valeur est 0 ou qu'il permute si la valeur est 1.

`Stop(0)` - Termine normalement la session en cours.

`Abort(0)` - Abandonne la session en cours.

Dans cet exemple, vous chargez la bande à partir de l'emplacement 3 (`SLOT 3`) sans permutation du support.

2. Tapez la commande permettant de charger la bande à partir de l'emplacement 3 (`SLOT 3`) sans permutation du support.

```
SLOT:LOAD 3 0
```

Une fois la bande chargée dans le lecteur, le message suivant s'affiche :

```
CHECK: [Deny(0), Init(1), Seek(2), Abort(0)]

CHECK: _
```

Les commandes disponibles sont les suivantes :

`Deny(0)`- Refuse l'action en cours.

`Init(1)`- Initialise la bande chargée et requiert un paramètre :

`Init(1)` *`ID_support`*

`Seek(2)`- Effectue une recherche à la position requise. La chaîne d'arguments est la suivante :

`Seek`*`numéro_segmentnuméro de bloc`*

`Abort(0)` - Abandonne la session en cours.

3. Pour initialiser la bande, tapez

   `CHECK: Init test`

4. Basculez de l'écran de l'Agent général de support de sauvegarde à la console Novell NetWare et démarrez la session de sauvegarde à l'aide de la commande d'action/de requête de l'Agent de support.

REMARQUE :

Vous devez démarrer l'Agent de disque Data Protector sur l'hôte sélectionné en entrant `load -ma` *`hôte port`* pour permettre une communication correcte entre l'Agent général de support et l'Agent de disque et afficher le bon numéro de port des opérations de la session de sauvegarde lorsque `HPCONMA.NLM` démarre. Une fois la session de sauvegarde terminée correctement, un message s'affiche.

5. Pour quitter correctement l'Agent de support de sauvegarde, appuyez sur **CTRL-C** lorsque l'écran de l'Agent de support de sauvegarde s'affiche. L'invite `Requête d'intervention sur la console` s'affiche au bout de quelques secondes :

   `ATT:[Stop(0), Abort(0), Disconnect(1)]` Exécutez la commande `Stop` pour terminer la session.

Test du démarrage de HPUMA.NLM et de HPDEVBRA.NLM

Le chargement de `HPUMA.NLM` sur la console du serveur permet de tester manuellement les commandes SCSI.

Chargez `HPUMA.NLM` à l'aide de la commande suivante :

```
LOAD HPUMA.NLM -ioctl périphérique_contrôle -dev
périphérique_données

-tty
```

L'option `ioctl` *`périphérique_contrôle`* définit l'adresse SCSI du contrôle du robot. Elle se présente sous la forme suivante :

`numéro_identification_adaptateur`:*`numéro_identification_cible`*:

`numéro_unité_logique`

comme l'illustre l'exemple suivant :

- `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`*

comme l'illustre l'exemple suivant :

- `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
```

D Modifications de la ligne de commande après la mise à niveau vers Data Protector 6.20

Les commandes répertoriées dans ce chapitre ont été modifiées ou proposent des fonctionnalités étendues concernant de nouvelles options dans Data Protector 6.20. Vérifiez et modifiez les scripts utilisant les anciennes commandes. Pour les synopsis d'utilisation, consultez le *Guide de référence de l'interface de ligne de commande HP Data Protector* ou les pages correspondantes du manuel.

Selon la version d'origine de la mise à niveau de votre Gestionnaire de cellule, reportez-vous au tableau correspondant :

- Pour la mise à niveau à partir de Data Protector A.06.00, reportez-vous au Tableau 13 à la page 471.
- Pour la mise à niveau à partir de Data Protector A.06.10, reportez-vous au Tableau 14 à la page 482.
- Pour la mise à niveau à partir de Data Protector A.06.11, reportez-vous au Tableau 15 à la page 489.
- Pour la mise à niveau à partir de Application Recovery Manager A.06.00, reportez-vous au Tableau 16 à la page 493.

Tableau 13 Mise à niveau à partir de Data Protector A.06.00

Commande	Options ou arguments affectés, notes	Etat
`cjutil`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Agent de disque` est installé.	NOUVELLE COMMANDE
`ob2install`	`chs_ls`	NOUVEAUX COMPOSANTS LOGICIELS
	`veagent`	

Commande	Options ou arguments affectés, notes	Etat
	vmware	
	vls_am	
	momgui	COMPOSANTS LOGICIELS OBSOLETES
	snapa	
omnib	-mssps_list	NOUVELLES INTEGRATIONS
	-vmware_list	
	-veagent_list	
	-mssharepoint_list	
	-e2010_list	
	-async	NOUVELLES OPTIONS
	-encode aes256	
	-clp	
	-resume	
	-ndmp_bkptype	
	-[no_]vss	NOUVELLE OPTION/OPTION MODIFIEE
omnicc	-encryption	NOUVELLES OPTIONS
	-enable	
	-cert	
	-key	

Commande	Options ou arguments affectés, notes	Etat
	-trust	
	-all	
	-add_exception	
	-remove_exception	
	-list_exceptions	
	-status	
	-add_certificate	
	-get_certificate	
	-list_certificates	
	-import_vls	
	-impersonation	
	-create_userrestrictions_tmpl	
	-port	OPTIONS MODIFIEES
	-user	
	-passwd	
omnicjutil	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE
omnicreatedl	-va	OPTIONS OBSOLETES
	-lun_security	
omnidb	-mssps	NOUVELLES INTEGRATIONS
	-vmware	

Commande	Options ou arguments affectés, notes	Etat
	-veagent	
	-e2010	
	-mssharepoint	
	-auditing	NOUVELLES OPTIONS
	-timeframe	
	–type verification	
	–encryptioninfo	
	–detail	OPTION MODIFIEE
omnidbcheck	-keystore	NOUVELLES OPTIONS
	-summary	
omnidbp4000	Cette commande est disponible sur les systèmes Windows sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omnidbrestore	–keyfile	NOUVELLE OPTION
omnidbsmis	-ompasswd -delete	NOUVELLE COMBINAISON D'OPTIONS
	-reference	NOUVELLES OPTIONS
	-sync_check	
	-exclude	
	-include	

Commande	Options ou arguments affectés, notes	Etat
	-namespace	OPTIONS OBSOLETES
	-sync	
omnidbutil	-free_cell_resources	NOUVELLES OPTIONS
	-list_large_directories	
	-list_large_mpos	
	-list_mpos_without_overs	
omnidbva		COMMANDE OBSOLETE
omnidbvss		COMMANDE REVUE
omnidlc	-add_info	NOUVELLES OPTIONS
	-pack	
	-no_config	
	–any	
	-del_tracelog	
omnihealthcheck	Sur les plates-formes Windows, cette commande a été déplacée du composant Interface utilisateur au package d'installation du Gestionnaire de cellule.	COMMANDE DEPLACEE
omniinetpasswd	Cette commande est disponible sur les systèmes sur lesquels un composant Data Protector est installé.	NOUVELLE COMMANDE
omniintconfig.pl	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE

Commande	Options ou arguments affectés, notes	Etat
omniiso	–autoinject	NOUVELLES OPTIONS
	-waik	
	-inject_drivers	
omnikeymigrate	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE
omnikeytool	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE
omnimcopy	–encrypt	NOUVELLES OPTIONS
	-ams	
	-copy	OPTIONS MODIFIEES
	-from	
	-pool	
omniminit	–ams	NOUVELLE OPTION
	–init	OPTIONS MODIFIEES
	–pool	
	–slot	
omnimm	-copy_to_mcf	NOUVELLES OPTIONS
	-import_from_mcf	
	-output_directory	
	-pool_prefix	
	-no_pool_prefix	

Commande	Options ou arguments affectés, notes	Etat
	-orig_pool	
	-no_orig_pool	
	–encryptioninfo	
	–ams	
omniobjconsolidate	–encrypt	NOUVELLE OPTION
omniobjcopy	–mssps	NOUVELLES INTEGRATIONS
	–vmware	
	-veagent	
	-e2010	
	-mssharepoint	
	–encrypt	NOUVELLES OPTIONS
	–restart	
	—sourceprotect	
	—targetprotect	
	–no_auto_device _selection	
	—protect	OPTIONS OBSOLETES
	—recycle	
	—no_recycle	

Commande	Options ou arguments affectés, notes	Etat
omniobjverify	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omnir	-mssps	NOUVELLES INTEGRATIONS
	-vmware	
	-veagent	
	-e2010	
	-mssharepoint	
	–no_auto_device _selection	NOUVELLES OPTIONS
	-omit_unrequired_object_versions	
	-resume	
	-[no_]resumable	
	-omit_unrequired_incrementals	OPTION OBSOLETE Remplacée par -omit_unrequired _object_versions.
	-appname	NOUVELLE OPTION Nouvelle option pour la restauration de Lotus Notes/Domino Server.

Commande	Options ou arguments affectés, notes	Etat
	-instant_restore	NOUVELLES OPTIONS Nouvelles options pour la restauration de VSS.
	-conf_check	
	-no_recovery	
	-use_vds	
	–no_copy_back	
	-copy_back	
	-diskarray_wait	
	-delete_replica	
	-no_diskarray_wait	
	-no_retain_source	
	–exch_check	
	-exch_throttle	
	-appsrv	
	-target_tree	
	–exch_RSG	
	-target_dir	
	-delete_current	OPTION OBSOLETE

Commande	Options ou arguments affectés, notes	Etat
	-stopat	NOUVELLE OPTION Nouvelle option pour la restauration de Microsoft SQL Server.
	-target Client	OPTION MODIFIEE Option modifiée pour la restauration du serveur NDMP.
	-copyback	NOUVELLES OPTIONS Nouvelles options pour HP StorageWorks P6000 EVA Disk Array Family.
	-switch	
	-leave_source	
	-no_leave_source	
	-no_check_config	
omnirpt	-copylist_sch	NOUVELLES OPTIONS
	-copylist_post	
	-conslist_sch	
	-conslist_post	
	-num_copies	
	-verificationlist_sch	
	-verificationlist_post	
	-no_verificationlist	

Commande	Options ou arguments affectés, notes	Etat
	-copylist	OPTIONS OBSOLETES
	-conslist	
	obj_copies	NOUVEAUX RAPPORTS
	session_objcopies	
	session_errors	
	session_statistics	
	backup_errors	RAPPORTS OBSOLETES
	backup_statistics	
omnisetup.sh	veagent	NOUVEAUX COMPOSANTS LOGICIELS
	chs_ls	
	docs	
	javagui	
	vls_am	
	vmware	
	momgui	COMPOSANTS LOGICIELS OBSOLETES
	snapa	
	-IS1	OPTIONS OBSOLETES
	-IS2	
omnistoreapputil	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE

Commande	Options ou arguments affectés, notes	Etat
omniusb	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Récupération automatique après sinistre est installé.	NOUVELLE COMMANDE
sanconf	-mom	NOUVELLE OPTION
uma	-vls_address	NOUVELLES OPTIONS
	-vls_port	
	-vls_username	
	-vls_password	
util_cmd	veagent	NOUVELLES INTEGRATIONS
	vmware	
	–encode	NOUVELLE OPTION

Tableau 14 Mise à niveau à partir de Data Protector A.06.10

Commande	Options ou arguments affectés, notes	Etat
ob2install	veagent	NOUVEAUX COMPOSANTS LOGICIELS
	vmware	
	chs_ls	
	snapa	COMPOSANT LOGICIEL OBSOLETE
omnib	–resume	NOUVELLES OPTIONS
	-ndmp_bkptype	

Commande	Options ou arguments affectés, notes	Etat
	-[no_]vss	NOUVELLE OPTION/OPTION MODIFIEE
	-veagent_list	NOUVELLES INTEGRATIONS
	-e2010_list	
	-mssharepoint_list	
	-clp	NOUVELLE COMBINAISON D'OPTIONS
omnicc	-encryption	NOUVELLES OPTIONS
	-enable	
	-cert	
	-key	
	-trust	
	-all	
	-add_exception	
	-remove_exception	
	-list_exceptions	
	-status	
	-add_certificate	
	-get_certificate	
	-list_certificates	

Commande	Options ou arguments affectés, notes	Etat
	-impersonation	
	-create_userrestrictions_tmpl	
omnicreatedl	-va	OPTIONS OBSOLETES
	-lun_security	
omnidb	-veagent	NOUVELLES INTEGRATIONS
	-e2010	
	-mssharepoint	
	–detail	OPTION MODIFIEE
	–encryptioninfo	NOUVELLES OPTIONS
	–type verification	
omnidbp4000	Cette commande est disponible sur les systèmes Windows sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omnidbsmis	-ompasswd -delete	NOUVELLE COMBINAISON D'OPTIONS
	-reference	NOUVELLES OPTIONS
	-sync_check	
	-exclude	
	-include	
	-namespace	OPTIONS OBSOLETES

Commande	Options ou arguments affectés, notes	Etat
	-sync	
omnidbva		COMMANDE OBSOLETE
omnidbvss	–get session_persistent	NOUVELLES OPTIONS
	-all	
	-details	
	-save_metadata	
	-disable session	
	–enable session	
	–mnttarget	
	–readwrite	
	–no_session_id	
	–backhost	
	–resolve	
	–get disk	OPTIONS OBSOLETES
	–list disk	
	–purge	
	–export_metadata	
omnihealthcheck	Sur les plates-formes Windows, cette commande a été déplacée du composant Interface utilisateur au package d'installation du Gestionnaire de cellule.	COMMANDE DEPLACEE

Commande	Options ou arguments affectés, notes	Etat
omniintconfig.pl	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omniminit	-ams	NOUVELLE OPTION
	-init	OPTIONS MODIFIEES
	-pool	
	-slot	
omnimm	-copy_to_mcf	NOUVELLES OPTIONS
	-import_from_mcf	
	-output_directory	
	-pool_prefix	
	-no_pool_prefix	
	-orig_pool	
	-no_orig_pool	
	-encryptioninfo	
	-ams	
	-show_locked_devs	
omniobjcopy	-veagent	NOUVELLES INTEGRATIONS
	-e2010	
	-mssharepoint	

Commande	Options ou arguments affectés, notes	Etat
	-restart	NOUVELLES OPTIONS
	-sourceprotect	
	-targetprotect	
	-no_auto_device _selection	
	-protect	OPTIONS OBSOLETES
	-recycle	
	-no_recycle	
omniobjverify	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omnir	-veagent	NOUVELLES INTEGRATIONS
	-e2010	
	-mssharepoint	
	-appname	NOUVELLE OPTION Nouvelle option pour la restauration de Lotus Notes/Domino Server.
	-resume	NOUVELLES OPTIONS
	-no_auto_device _selection	

Commande	Options ou arguments affectés, notes	Etat
	–newinstance "None"	NOUVELLE VALEUR D'OPTION Nouvelle valeur d'option pour le composant Intégration VMware (hérité) de Data Protector.
	–no_auto_dev	OPTION OBSOLETE Remplacée par –no_auto_device_selection
	-stopat	NOUVELLE OPTION Nouvelle option pour la restauration de Microsoft SQL Server.
	-copyback	NOUVELLES OPTIONS Nouvelles options pour HP StorageWorks P6000 EVA Disk Array Family.
	-switch	
	-leave_source	
	-no_leave_source	
	-no_check_config	
	-target Client	OPTION MODIFIEE Option modifiée pour la restauration du serveur NDMP.

Commande	Options ou arguments affectés, notes	Etat
omnirpt	-verificationlist_sch	NOUVELLES OPTIONS
	-verificationlist_post	
	-no_verificationlist	
omnisetup.sh	veagent	NOUVEAUX COMPOSANTS LOGICIELS
	vmware	
	chs_ls	
	snapa	COMPOSANT LOGICIEL OBSOLETE
omniusb	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Récupération automatique après sinistre est installé.	NOUVELLE COMMANDE
sanconf	–mom	NOUVELLE OPTION
util_cmd	veagent	NOUVELLES INTEGRATIONS
	vmware	
	–encode	NOUVELLE OPTION

Tableau 15 Mise à niveau à partir de Data Protector A.06.11

Commande	Options ou arguments affectés, notes	Etat
ob2install	veagent	NOUVEAUX COMPOSANTS LOGICIELS
	chs_ls	

Commande	Options ou arguments affectés, notes	Etat
	snapa	COMPOSANT LOGICIEL OBSOLETE
omnib	-clp	NOUVELLE COMBINAISON D'OPTIONS
	-veagent_list	NOUVELLES INTEGRATIONS
	-e2010_list	
	-mssharepoint_list	
omnicc	-encryption	NOUVELLES OPTIONS
	-enable	
	-cert	
	-key	
	-trust	
	-all	
	-add_exception	
	-remove_exception	
	-list_exceptions	
	-status	
	-add_certificate	
	-get_certificate	
	-list_certificates	

Commande	Options ou arguments affectés, notes	Etat
	-impersonation	
	-create_userrestrictions_tmpl	
omnicreatedl	-va	OPTIONS OBSOLETES
	-lun_security	
omnidb	-veagent	NOUVELLES INTEGRATIONS
	-e2010	
	-mssharepoint	
omnidbp4000	Cette commande est disponible sur les systèmes Windows sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omnidbsmis	-ompasswd -delete	NOUVELLE COMBINAISON D'OPTIONS
	-reference	NOUVELLES OPTIONS
	-sync_check	
	-exclude	
	-include	
	-namespace	OPTIONS OBSOLETES
	-sync	
omnidbva		COMMANDE OBSOLETE
omnimm	-show_locked_devs	NOUVELLES OPTIONS

Commande	Options ou arguments affectés, notes	Etat
	-all	
omniobjcopy	-veagent	NOUVELLES INTEGRATIONS
	-e2010	
	-mssharepoint	
omniobjverify	-veagent	NOUVELLES INTEGRATIONS
	-e2010	
	-mssharepoint	
omnir	-veagent	NOUVELLES INTEGRATIONS
	-e2010	
	-mssharepoint	
	-copyback	NOUVELLES OPTIONS Nouvelles options pour HP StorageWorks P6000 EVA Disk Array Family.
	-switch	
	-leave_source	
	-no_leave_source	
	-no_check_config	
omnirsh	-add	NOUVELLE COMMANDE
	-modify	
omnisetup.sh	veagent	NOUVEAUX COMPOSANTS LOGICIELS
	chs_ls	

Commande	Options ou arguments affectés, notes	Etat
	`snapa`	COMPOSANT LOGICIEL OBSOLETE
`omniusb`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Récupération automatique après sinistre` est installé.	NOUVELLE COMMANDE
`util_cmd`	`veagent`	NOUVELLE INTEGRATION

Tableau 16 Mise à niveau à partir de Application Recovery Manager A.06.00

Commande	Options ou arguments affectés, notes	Etat
`omnib`	`-disk_only`	NOUVELLE OPTION Nouvelle option pour sauvegarde ZDB sur disque.
	Nouvelles options d'intégrations et de système de fichiers.	NOUVELLES OPTIONS
`omnidb`	Nouvelles options relatives à la gestion des supports et autre nouvelle fonctionnalité de Data Protector.	NOUVELLES OPTIONS
`omnidbp4000`	Cette commande est disponible sur les systèmes Windows sur lesquels le composant Data Protector `Interface utilisateur` est installé.	NOUVELLE COMMANDE
`omnidbsmis`	`-host`	NOUVELLES OPTIONS
	`-dgrules`	
	`-init`	
	`-put`	

Commande	Options ou arguments affectés, notes	Etat
	-get	
	-caconf	
	-session	
	-ir	
	-excluded	
	-original	
	-datalist	
	-show	
	-purge	
	-force	
	-delete	
	-preview	
	-sync	
	-reference	
	-sync_check	
	-exclude	
	-include	
	-ompasswd -delete	NOUVELLE COMBINAISON D'OPTIONS
	-namespace	OPTIONS OBSOLETES

Commande	Options ou arguments affectés, notes	Etat
	-sync	
omnidbutil	Nouvelles options relatives à la gestion des supports et autre nouvelle fonctionnalité de Data Protector.	NOUVELLES OPTIONS
omnidbvss	–get session_persistent	NOUVELLES OPTIONS
	–list session_persistent	
	–remove session_persistent	
	-all	
	-details	
	-save_metadata	
	-disable session	
	–enable session	
	–mnttarget	
	–readwrite	
	–no_session_id	
	–backhost	
	–resolve	
	–get disk	OPTIONS OBSOLETES
	–list disk	
	–remove disk	
	–purge	

Commande	Options ou arguments affectés, notes	Etat
	`-export_metadata`	
`omnihealthcheck`	Cette commande a été déplacée du composant Interface utilisateur au package d'installation du Gestionnaire de cellule.	COMMANDE DEPLACEE
`omnir`	Nouvelles options d'intégrations et de système de fichiers. Les options d'Application Recovery Manager A.06.00 sont disponibles. Pour plus d'informations, reportez-vous au *Guide de référence de l'interface de ligne de commande HP Data Protector*.	UTILISATION DE COMMANDE REVUE
`dbtool.pl`	La fonctionnalité de commande a été remplacée par la sauvegarde de base de données interne.	COMMANDE OBSOLETE
REMARQUE : La première partie de la table recense uniquement les modifications apportées aux commandes déjà disponibles dans Application Recovery Manager A.06.00 et qui peuvent affecter vos scripts. Toutes les commandes *introduites avec Data Protector* sont indiquées ci-dessous comme nouvelles commandes.		
`cjutil`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Agent de disque` est installé.	NOUVELLE COMMANDE
`NNMpost.ovpl`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Intégration de HP Network Node Manager` est installé.	NOUVELLE COMMANDE
`NNMpre.ovpl`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Intégration de HP Network Node Manager` est installé.	NOUVELLE COMMANDE

Commande	Options ou arguments affectés, notes	Etat
NNMScript.exe	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Intégration de HP Network Node Manager est installé.	NOUVELLE COMMANDE
ob2install	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE
omniamo	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE
omnicjutil	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE
omnicreatedl	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omnidbrestore	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE
omnidbupgrade	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE
omnidbxp	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omnidownload	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omnidr	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE

Commande	Options ou arguments affectés, notes	Etat
`omniinetpasswd`	Cette commande est disponible sur les systèmes sur lesquels un composant Data Protector est installé.	NOUVELLE COMMANDE
`omniintconfig.pl`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Interface utilisateur` est installé.	NOUVELLE COMMANDE
`omniiso`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Récupération automatique après sinistre` est installé.	NOUVELLE COMMANDE
`omnikeymigrate`	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE
`omnikeytool`	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE
`omnimcopy`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Interface utilisateur` est installé.	NOUVELLE COMMANDE
`omnimigrate.pl`	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE
`omniminit`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Interface utilisateur` est installé.	NOUVELLE COMMANDE
`omnimlist`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Interface utilisateur` est installé.	NOUVELLE COMMANDE
`omnimm`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Interface utilisateur` est installé.	NOUVELLE COMMANDE

Commande	Options ou arguments affectés, notes	Etat
omnimnt	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omnimver	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omniobjconsolidate	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omniobjcopy	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omniobjverify	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omniofflr	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omniresolve	Cette commande est disponible sur les systèmes sur lesquels un composant d'intégration Data Protector est installé.	NOUVELLE COMMANDE
omnirpt	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector Interface utilisateur est installé.	NOUVELLE COMMANDE
omnirsh	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE

Commande	Options ou arguments affectés, notes	Etat
`omnisetup.sh`	Cette commande est disponible sur les DVD-ROM d'installation de Data Protector pour les systèmes UNIX.	NOUVELLE COMMANDE
`omnisrdupdate`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Interface utilisateur` est installé.	NOUVELLE COMMANDE
`omniupload`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Interface utilisateur` est installé.	NOUVELLE COMMANDE
`omniusb`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Récupération automatique après sinistre` est installé.	NOUVELLE COMMANDE
`omniusers`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Interface utilisateur` est installé.	NOUVELLE COMMANDE
`sanconf`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Interface utilisateur` est installé.	NOUVELLE COMMANDE
`syb_tool`	Cette commande est disponible sur les systèmes sur lesquels le composant Data Protector `Interface utilisateur` est installé.	NOUVELLE COMMANDE
`uma`	Cette commande est disponible sur les systèmes sur lesquels le composant `Agent général de support` ou `Agent de support NDMP` Data Protector est installé.	NOUVELLE COMMANDE
`upgrade_cm_from_evaa`	Cette commande est disponible sur le Gestionnaire de cellule Data Protector.	NOUVELLE COMMANDE

Commande	Options ou arguments affectés, notes	Etat
`util_cmd`	Cette commande est disponible sur les systèmes sur lesquels un composant Data Protector est installé.	NOUVELLE COMMANDE
`util_oracle8.pl`	Cette commande est disponible sur les systèmes sur lesquels le composant `Intégration Oracle` Data Protector est installé.	NOUVELLE COMMANDE
`util_vmware.exe`	Cette commande est disponible sur les systèmes sur lesquels le composant `Intégration VMware` Data Protector est installé.	NOUVELLE COMMANDE

Glossaire

ACSLS

(terme propre à StorageTek) Automated Cartridge System Library Server (ACSLS), serveur de bibliothèque à système de cartouche automatisé - logiciel chargé de la gestion du système de cartouche automatisé (ACS).

Active Directory

(terme propre à Windows) Service d'annuaire d'un réseau Windows. Il contient des informations sur les ressources du réseau et les rend accessibles aux utilisateurs et aux applications. Les services d'annuaire permettent de nommer, de décrire, de localiser, de consulter et de gérer les ressources de manière cohérente, quel que soit le système physique sur lequel elles résident.

affichage de sauvegarde

Data Protector propose plusieurs affichages pour les spécifications de sauvegarde :
Par type - en fonction du type de données disponibles pour les sauvegardes ou les modèles. Affichage par défaut.
Par groupe - en fonction du groupe auquel les spécifications/modèles de sauvegarde appartiennent.
Par nom - en fonction du nom des spécifications/modèles de sauvegarde.
Par gestionnaire - si vous utilisez le MoM, vous pouvez également définir l'affichage de sauvegarde en fonction du Gestionnaire de cellule auquel appartiennent les spécifications/modèles de sauvegarde.

agent d'application

Composant requis sur un client pour sauvegarder ou restaurer les intégrations de bases de données en ligne.
Voir aussi Agent de disque.

Agent de disque

Composant devant être installé sur un client pour que ce dernier puisse être sauvegardé et restauré. L'Agent de disque contrôle la lecture et l'écriture de données sur un disque. Pendant une session de sauvegarde, l'Agent de disque lit les données

stockées sur un disque et les envoie à l'Agent de support qui les déplace ensuite vers le périphérique. Pendant une session de restauration, l'Agent de disque reçoit des données de l'Agent de support et les écrit sur le disque. Au cours d'une session de vérification d'objet, l'Agent de disque reçoit des données de l'Agent de support et exécute le processus de vérification, mais aucune donnée n'est écrite sur le disque.

Agent de support Processus contrôlant la lecture et l'écriture de données sur un périphérique qui lui-même lit ou écrit des données sur un support (généralement une bande). Pendant une session de sauvegarde, un Agent de support reçoit des données de l'Agent de disque et les envoie au périphérique qui les écrit ensuite sur le support. Lors d'une session de restauration ou de vérification d'objet, un Agent de support localise les données stockées sur le support de sauvegarde et les envoie à l'Agent de disque en vue de leur traitement. Lors d'une session de restauration, l'Agent de disque écrit les données sur le disque. Un Agent de support gère également le contrôle robotique d'une bibliothèque.

Agent EMC Symmetrix Module logiciel Data Protector qui prépare l'environnement EMC Symmetrix aux opérations de sauvegarde et de restauration.

Agent HP StorageWorks P6000 EVA SMI-S Module logiciel de Data Protector qui exécute toutes les tâches nécessaires à l'intégration HP StorageWorks P6000 EVA Disk Array Family. Avec l'Agent P6000 EVA SMI-S, le contrôle sur la baie est assuré par le fournisseur HP StorageWorks SMI-S P6000 EVA Array qui dirige la communication entre les demandes entrantes et HP StorageWorks CV EVA.
Voir aussi HP StorageWorks Command View (CV) EVA et fournisseur HP StorageWorks SMI-S P6000 EVA Array.

Agent HP StorageWorks P9000 XP Composant logiciel de Data Protector qui exécute toutes les tâches nécessaires à l'intégration de Data Protector avec HP StorageWorks P9000 XP Disk Array Family. Il communique avec le système de stockage P9000 XP Array à l'aide de l'utilitaire Gestionnaire RAID P9000 XP (sur les systèmes HP-UX et Windows) ou de la bibliothèque du Gestionnaire RAID (sur les systèmes Solaris).

Agent SSE (SSEA) ***(terme propre à HP*** *Voir* Agent HP StorageWorks P9000 XP.

P9000 XP Array Family)

Agents de disque simultanés Nombre d'Agents de disque autorisés à envoyer des données simultanément à un Agent de support.

AML *(terme propre à ADIC/GRAU)* Automated Mixed-Media library, bibliothèque de supports mixtes automatisée.

AMU *(terme propre à ADIC/GRAU)* Archive Management Unit, unité de gestion d'archive.

analyse Fonction permettant d'identifier les supports contenus dans un périphérique. Cette fonction synchronise la MMDB avec les supports se trouvant aux emplacements sélectionnés (les logements d'une bibliothèque, par exemple). Elle est utile pour analyser et vérifier le support effectivement présent dans le périphérique lorsque quelqu'un a manipulé le support manuellement sans utiliser Data Protector pour l'éjecter ou l'insérer, par exemple.

API C Lotus *(terme propre à Lotus Domino Server)* Interface destinée à l'échange de données de sauvegarde et de récupération entre Lotus Domino Server et une solution de sauvegarde comme Data Protector.

API de sauvegarde Programme Oracle servant d'interface entre l'utilitaire de sauvegarde/restauration d'Oracle et la couche de gestion des supports de sauvegarde/restauration. L'interface définit un ensemble de routines afin de permettre la lecture et l'écriture des données sur les supports de sauvegarde, ainsi que la création, la recherche et la suppression des fichiers de sauvegarde.

API de serveur de sauvegarde Sybase *(terme propre à Sybase)* Interface standard développée pour l'échange de données de sauvegarde et de récupération entre un serveur Sybase SQL et une solution de sauvegarde telle que Data Protector.

application compatible cluster Application prenant en charge l'API cluster (Application Programming Interface). Chaque application compatible cluster déclare ses propres ressources stratégiques (volumes de disques (sous Microsoft Cluster Server), groupes de volumes (sous

MC/ServiceGuard), services d'application, noms et adresses IP, etc.).

archivage des journaux

(terme propre à Lotus Domino Server) Mode de connexion à la base de données Lotus Domino Server qui permet de n'écraser les fichiers journaux de transactions qu'après leur sauvegarde.

auto-migration

(terme propre à VLS) Fonctionnalité qui permet de procéder initialement à la sauvegarde des données sur les bandes virtuelles des VLS, puis de les faire migrer vers des bandes physiques (une bande virtuelle émulant une bande physique) sans utiliser d'application de sauvegarde intermédiaire.
Voir aussi Système de bibliothèque virtuelle (VLS) et bande virtuelle.

BACKINT

(terme propre à SAP R/3) Par le biais d'une interface ouverte, les programmes de sauvegarde SAP R/3 peuvent appeler l'interface backint Data Protector, laquelle leur permet de communiquer avec le logiciel Data Protector. En ce qui concerne la restauration et la sauvegarde, les programmes SAP R/3 émettent des ordres destinés à l'interface backint Data Protector.

bande virtuelle

(terme propre à VLS) Technologie d'archivage qui sauvegarde les données sur des lecteurs de disque de la même manière que si elles étaient stockées sur bande. Les systèmes de bandes virtuelles permettent daccélérer les processus de sauvegarde et de restauration et de réduire les coûts de fonctionnement.
Voir aussi système de bibliothèques virtuelles (VLS) et bibliothèque de bandes virtuelle.

banque d'informations

(terme propre à Microsoft Exchange Server) Service de Microsoft Exchange Server chargé de la gestion du stockage. La banque d'informations de Microsoft Exchange Server gère deux types de banques : les boîtes aux lettres et les dossiers publics. Une banque de boîtes aux lettres est constituée de boîtes aux lettres appartenant à des utilisateurs individuels. Une banque d'informations publiques contient des dossiers et des messages publics partagés entre plusieurs utilisateurs.
Voir aussi service Gestionnaire de clés et service de réplication de sites.

banque de boîtes aux lettres

(terme propre à Microsoft Exchange Server) Partie de la banque d'informations conservant les informations se trouvant dans les boîtes aux lettres des utilisateurs. Une banque de boîtes aux

lettres est constituée d'un fichier binaire RTF `.edb` et d'un fichier de contenu Internet natif continu `.stm`.

banque de clés

Toutes les clés de cryptage sont stockées de manière centralisée dans la banque de clés sur le Gestionnaire de cellule et sont gérées par le serveur gestionnaire de clés (KMS).

banque de dossiers publics

(terme propre à Microsoft Exchange Server) Partie de la banque d'informations conservant les informations se trouvant dans les dossiers publics. Une banque de dossiers publics est constituée d'un fichier binaire RTF `.edb` et d'un fichier de contenu Internet natif continu `.stm`.

basculement

Transfert des données de cluster les plus importantes, également appelées groupe (Windows) ou package (UNIX), d'un nœud de cluster à un autre. Un basculement peut se produire en raison de défaillances logicielles ou matérielles, ou d'opérations de maintenance au niveau du nœud primaire.

basculement

(terme propre à HP P6000 EVA Array Family) Opération qui renverse les rôles entre source et destination dans les configurations HP Continuous Access + Business Copy (CA + BC) P6000 EVA.
Voir aussi HP Continuous Access + Business Copy (CA + BC) P6000 EVA.

Base de données centralisée de gestion des supports (CMMDB)

Voir CMMDB.

base de données cible

(terme propre à Oracle) Terme utilisé dans le contexte du Gestionnaire de récupération (RMAN). La base de données cible est celle qui est sauvegardée ou restaurée.

Base de données d'enregistrement des classes COM+

(terme propre Windows) La base de données de registres de classe COM+ et la base de registres Windows stockent les attributs d'applications, de classes et de matériels COM+. Elles garantissent ainsi la cohérence entre ces attributs et assurent un fonctionnement courant pour gérer ces derniers.

base de données du catalogue de récupération

(terme propre à Oracle) Base de données Oracle contenant un schéma de catalogue de récupération. Il est recommandé de

ne pas stocker le catalogue de récupération dans la base de données cible.

Base de données du gestionnaire de supports amovibles

(terme propre à Windows) Service Windows pour la gestion de supports amovibles (tels que des bandes et des disques) et de périphériques de stockage (bibliothèques). Le stockage sur supports amovibles permet aux applications d'accéder aux ressources de mêmes supports et de les partager.

base de données ZDB

(terme propre à la sauvegarde ZDB) Partie de la base de données interne stockant des informations sur la sauvegarde ZDB, telles que les volumes sources, les répliques et les données de sécurité. La base de données ZDB est utilisée pour la sauvegarde avec temps d'indisponibilité nul, la restauration instantanée et la restauration Split Mirror.
Voir aussi sauvegarde avec temps d'indisponibilité nul (ZDB).

bases de données système

(terme propre à Sybase) Les quatre bases de données système d'un Sybase SQL Server nouvellement installé sont les suivantes :

- base de données principale (master)
- base de données temporaire (tempdb)
- base de données de procédures système (sybsystemprocs)
- base de données modèle (model)

BC

(terme propre à EMC Symmetrix) Business Continuance - Procédé permettant aux utilisateurs d'accéder et de gérer des copies instantanées des périphériques standard EMC Symmetrix.
Voir aussi BCV.

BCV

*(terme propre à EMC Symmetrix)*Business Continuance Volumes ou périphériques BCV - il s'agit de SLD dédiés, préconfigurés dans l'ICDA sur lequel l'opération Business Continuance est exécutée. Des adresses SCSI distinctes, lesquelles diffèrent des adresses utilisées par les SLD dont elles sont le miroir, sont attribuées aux périphériques BCV. Ces derniers sont utilisés comme miroirs séparables des SLD EMC Symmetrix principaux devant être protégés.
Voir aussi BC et Processus BC.

bibliothèque

Egalement appelée "changeur automatique", "bibliothèque de banques magnéto-optiques", "chargeur automatique" ou "échangeur". Une bibliothèque contient des supports stockés dans des emplacements référentiels. Chaque emplacement

contient un support (par exemple, DDS/DAT). Les supports sont déplacés entre les emplacements et les lecteurs par un mécanisme robotique permettant un accès aléatoire aux supports. Une bibliothèque peut contenir plusieurs lecteurs.

bibliothèque de bandes magnéto-optiques

Voir bibliothèque.

bibliothèque de bandes virtuelle (VTL)

(terme propre à VLS) Emulation de bibliothèque de bandes fournissant les mêmes fonctionnalités qu'un stockage sur bandes traditionnel.
Voir aussi système de bibliothèques virtuelles (VLS).

bibliothèque de base de données

Ensemble de routines Data Protector permettant le transfert de données entre Data Protector et le serveur d'une intégration de base de données en ligne, le serveur Oracle par exemple.

bibliothèque du Gestionnaire RAID

(terme propre à HP P9000 XP Array Family) Bibliothèque utilisée en interne par Data Protector sur les systèmes Solaris pour permettre l'accès aux données de configuration, d'état et de performances de HP StorageWorks P9000 XP Disk Array Family, ainsi qu'aux fonctions clés de HP StorageWorks P9000 XP Disk Array Family au moyen d'appels de fonction convertis en une séquence de commandes SCSI de bas niveau.

bibliothèque StorageTek ACS

(terme propre à StorageTek) Système de bibliothèque (également connu sous le nom de "silo") constitué d'une unité de gestion de bibliothèque (LMU) et d'un à vingt-quatre modules de stockage en bibliothèque (LSM) connectés à l'unité.

boîte aux lettres

(terme propre à Microsoft Exchange Server) Emplacement où sont livrés les messages électroniques. Cet emplacement est défini par l'administrateur pour chaque utilisateur. Si un ensemble de dossiers personnels est désigné comme emplacement de distribution du courrier électronique, les messages sont acheminés de la boîte aux lettres vers cet emplacement.

BRARCHIVE

(terme propre à SAP R/3) Outil de sauvegarde SAP R/3 permettant à l'utilisateur d'archiver les fichiers journaux de rétablissement. BRARCHIVE permet également d'enregistrer l'ensemble des journaux et profils du processus d'archivage.
Voir aussi BRBACKUP et BRRESTORE.

BRBACKUP

(terme propre à SAP R/3) Outil de sauvegarde SAP R/3 permettant d'effectuer une sauvegarde en ligne ou hors ligne du fichier de contrôle, de fichiers de données distincts ou de l'ensemble des espaces de tables et, le cas échéant, des fichiers journaux de rétablissement en ligne.
Voir aussi BRARCHIVE et BRRESTORE.

BRRESTORE

(terme propre à SAP R/3) Outil de sauvegarde SAP R/3 pouvant être utilisé pour restaurer les types de fichiers suivants :

- fichiers de données de base de données, fichiers de contrôle et fichiers journaux de rétablissement en ligne sauvegardés avec BRBACKUP
- fichiers journaux de rétablissement archivés avec BRARCHIVE
- fichiers "non-base de données" sauvegardés avec BRBACKUP

Vous pouvez spécifier des fichiers, des espaces de table, des sauvegardes complètes, des numéros de séquence de fichiers journaux de rétablissement ou l'ID de session de la sauvegarde.
Voir aussi BRBACKUP et BRARCHIVE.

BSM

Le Backup Session Manager Data Protector (Gestionnaire de session de sauvegarde) contrôle la session de sauvegarde. Ce processus est toujours exécuté sur le système du Gestionnaire de cellule.

canal

(terme propre à Oracle) Allocation de ressources du Gestionnaire de récupération Oracle. Chaque canal alloué lance un nouveau processus Oracle qui effectue des opérations de sauvegarde, de restauration et de récupération. Le type de canal affecté détermine le type de support utilisé :

- type 'disk'
- type ‘sbt_tape’

Si le canal spécifié est de type ‘sbt_tape’ et qu'Oracle est intégré avec Data Protector, le processus du serveur essaie de lire les sauvegardes ou d'écrire les fichiers de données sur Data Protector.

CAP

(terme spécifique à StorageTek) Cartridge Access Port - port d'accès intégré au panneau porte d'une bibliothèque permettant d'insérer ou d'éjecter les supports.

caractère générique

Caractère pouvant être utilisé pour représenter un ou plusieurs caractères. Par exemple, l'astérisque (*) représente généralement un ou plusieurs caractères et le point d'interrogation (?) un seul caractère. Les caractères génériques sont souvent utilisés avec les systèmes d'exploitation pour spécifier plusieurs fichiers par nom.

catalogue de récupération

(terme propre à Oracle) Ensemble de tables et de vues Oracle permettant au Gestionnaire de récupération de stocker des informations sur les bases de données Oracle. Grâce à ces informations, le Gestionnaire de récupération peut gérer la sauvegarde, la restauration et la récupération des bases de données Oracle. Le catalogue de récupération contient des informations sur :

- le schéma physique de la base de données cible Oracle,
- les jeux de sauvegarde de fichiers de données et de journaux d'archive,
- les copies de fichiers de données,
- les journaux de rétablissement archivés,
- les scripts stockés.

CDB

La base de données catalogue est une partie de la base de données IDB qui contient des informations sur les sessions de sauvegarde, de restauration, de copie d'objet, de consolidation d'objet, de vérification d'objet et de gestion de support. En fonction du niveau de journalisation sélectionné, la CDB contient également les noms et versions de fichiers. Cette partie de la base de données se trouve toujours dans la cellule locale. *Voir aussi* MMDB.

cellule

Ensemble de systèmes contrôlés par un Gestionnaire de cellule. Une cellule représente généralement les systèmes d'un site ou d'une entité organisationnelle connectés au même réseau local/SAN. Un contrôle centralisé permet d'administrer les tâches et les stratégies de sauvegarde et de restauration.

Certificate Server

Un Certificate Server (ou serveur de certificats) Windows peut être installé et configuré pour fournir des certificats aux clients. Il propose des services personnalisables d'émission et de gestion de certificats pour l'entreprise. Ces services permettent d'émettre, de résilier et de gérer les certificats utilisés dans les technologies de cryptographie à clé publique.

chaîne de périphériques
Série de périphériques autonomes configurés pour une utilisation séquentielle. Lorsqu'un support est plein dans un périphérique, la sauvegarde se poursuit automatiquement sur un support du périphérique suivant dans la chaîne de périphériques.

chaîne de restauration
Toutes les sauvegardes nécessaires à la restauration d'un objet sauvegarde à un point dans le temps donné (version). Une chaîne de restauration consiste en une sauvegarde complète de l'objet et un certain nombre de sauvegardes incrémentales liées.

chaîne de sauvegarde
Voir chaîne de restauration.

changeur automatique
Voir bibliothèque.

chargeur automatique
Voir bibliothèque.

chargeurs
Périphériques possédant plusieurs emplacements destinés au stockage des supports et disposant généralement d'un seul lecteur. Un chargeur sélectionne les supports dans une pile de manière séquentielle. Une bibliothèque, en revanche, peut sélectionner les supports de manière aléatoire depuis son référentiel.

clé de cryptage
Un numéro 256 bits généré au hasard utilisé par l'algorithme de cryptage Data Protector pour coder des informations pendant les sauvegardes pour lesquelles le cryptage sur logiciel ou sur lecteur 256 bits a été spécifié. La même clé sert au décryptage ultérieur des informations. Les clés de cryptage pour une cellule Data Protector sont stockées dans une banque de clés centrale dans le Gestionnaire de cellule.

clé de session
Cette variable d'environnement pour les scripts de pré-exécution et de post-exécution constitue une identification unique de session dans Data Protector, y compris pour les sessions de test. La clé de session n'est pas enregistrée dans la base de données ; elle permet de spécifier les options relatives aux commandes `omnimnt`, `omnistat` et `omniabort`.

client d'interface Java
Le client d'interface Java est un composant de l'interface utilisateur graphique Java qui contient uniquement les

fonctionnalités liées à l'interface utilisateur (interface utilisateur graphique du Gestionnaire de cellule et interface utilisateur graphique du Manager-of-Managers (MoM)) et qui doit être connecté au serveur d'interface Java pour fonctionner.

client de gestion VMware

(terme propre à l'intégration VMware (hérité)) Client utilisé par Data Protector pour communiquer avec l'infrastructure virtuelle VMware. Il peut s'agir d'un système VirtualCenter Server (environnement VirtualCenter) ou d'un système ESX Server (environnement autonome ESX Server).

client ou système client

Tout système configuré avec des fonctions Data Protector et dans une cellule.

Cluster Continuous Replication

(terme propre à Microsoft Exchange Server) Cluster Continuous Replication (CCR) est une solution de haute disponibilité qui fait appel à des options de gestion des clusters et de basculement pour créer et conserver une copie exacte (copie CCR) d'un groupe de stockage. Un groupe de stockage est répliqué sur un serveur distinct. CCR supprime tous les points de défaillance de vos serveurs de back-end Exchange. Vous pouvez procéder à des sauvegardes à l'aide de VSS sur le noeud Exchange Server passif qui contient une copie CCR, de telle sorte à réduire la charge sur le noeud actif.
Les copies CCR servent à des fins de récupération après sinistre, puisqu'il est possible de basculer sur la copie CCR en quelques secondes. Un groupe de stockage répliqué est représenté comme une nouvelle instance du module d'écriture Exchange nommé Service de réplication Exchange et peut être sauvegardé (à l'aide de VSS) comme n'importe quel groupe de stockage.
Voir aussi Service de réplication Exchange et Local Continuous Replication.

CMMDB

Centralized Media Management Database, base de données centralisée de gestion des supports - La CMMDB Data Protector résulte de la fusion des bases de données de gestion des supports à partir de plusieurs cellules dans l'environnement MoM. Elle permet à l'utilisateur de partager des supports et périphériques haut de gamme avec plusieurs cellules dans un environnement MoM. Une cellule peut contrôler les systèmes robotiques desservant les périphériques connectés à des systèmes se trouvant dans d'autres cellules. La CMMDB doit résider sur le Manager-of-Managers. Une connexion réseau

fiable entre la cellule MoM et les autres cellules Data Protector est vivement recommandée.
Voir aussi MoM.

Command View VLS

(terme propre à VLS) Interface utilisateur graphique sur le Web servant à configurer, à gérer et à surveiller le VLS sur un réseau local.
Voir aussi système de bibliothèques virtuelles (VLS).

commandes pré- et post-exécution

Les commandes pré- et post-exécution servent à réaliser une action supplémentaire avant et après une session de sauvegarde ou de restauration. Elles ne sont pas fournies avec Data Protector. L'utilisateur doit les créer lui-même. Elles peuvent être rédigées sous la forme de programmes exécutables ou de fichiers séquentiels sous Windows, ou bien de scripts shell sous UNIX.

communications de contrôle cryptées

Data Protector sécurise les échanges entre les clients de la cellule Data Protector, sur la base du protocole SSL (Secure Socket Layer) qui utilise des algorithmes SSLv3 pour crypter les communications de contrôle. Les communications de contrôle dans une cellule Data Protector correspondent à tous les échanges entre les processus Data Protector, à l'exception du transfert de données de l'Agent de disque (et des intégrations) vers l'Agent de support, et vice versa.

compte utilisateur (compte utilisateur Data Protector)

Vous ne pouvez utiliser Data Protector que si vous disposez d'un compte utilisateur Data Protector, lequel limite l'accès non autorisé à Data Protector et aux données sauvegardées. Les administrateurs de Data Protector créent ce compte en spécifiant un nom d'utilisateur, les systèmes à partir desquels l'utilisateur peut se connecter et le groupe d'utilisateurs Data Protector auquel il sera affecté. Ces éléments sont vérifiés chaque fois que l'utilisateur démarre l'interface utilisateur de Data Protector ou effectue certaines tâches.

consolidation d'objet

Processus permettant de fusionner une chaîne de restauration d'un objet sauvegarde, comprenant une sauvegarde complète et au moins une sauvegarde incrémentale, en une nouvelle version consolidée de cet objet. Ce processus fait partie de la procédure de sauvegarde synthétique. Le résultat est une sauvegarde complète synthétique de l'objet sauvegarde spécifié.

conteneur *(terme propre à HP P6000 EVA Array Family)* Espace sur une baie de disques qui est préalloué pour une utilisation ultérieure en tant que snapshot standard, vsnap ou snapclone.

contrôleur de domaine Serveur d'un réseau responsable de la sécurité de l'utilisateur et de la vérification des mots de passe dans un groupe d'autres serveurs.

copie d'objet Copie d'une version spécifique d'un objet créé au cours d'une session de copie d'objets ou de sauvegarde avec la fonction de mise en miroir d'objets.

copie intelligente *(terme propre à VLS)* Copie des données sauvegardées créée à partir de la bande virtuelle vers la bibliothèque de bandes physiques. Le processus smart copy (copie intelligente) permet à Data Protector d'établir une distinction entre les supports source et cible, et ainsi de gérer les supports.
Voir aussi système de bibliothèques virtuelles (VLS).

copie miroir *(terme propre à Microsoft VSS)* Volume représentant une copie du volume d'origine à un instant donné. La sauvegarde de données s'effectue alors depuis la copie miroir, et non depuis le volume d'origine. Le volume d'origine change à mesure que le processus de sauvegarde se poursuit ; la copie miroir, en revanche, demeure identique.
Voir aussi Microsoft Volume Shadow Copy Service et réplique.

création de réplique Split Mirror *(terme propre à EMC Symmetrix et à HP P9000 XP Array Family)* Technique de création de réplique selon laquelle un ensemble de volumes cibles pré-configuré (un miroir) est synchronisé en permanence avec un ensemble de volumes sources jusqu'à ce qu'une réplique du contenu des volumes sources soit requise. La synchronisation est alors arrêtée (le miroir est séparé) et une réplique Split Mirror des volumes sources au moment de la séparation est conservée dans les volumes cibles.
Voir aussi Split Mirror.

création de snapshot *(terme propre à HP P6000 EVA Array Family, HP P9000 XP Array Family et HP StorageWorks P4000 SAN Solutions)* Processus de création de réplique permettant de générer des copies de volumes sources sélectionnés au moyen de technologies de virtualisation du stockage. Une telle réplique est considérée comme créée à un moment donné et elle est disponible immédiatement. Toutefois, avec certains types de

snapshots, un processus de copie des données en arrière-plan continue de s'exécuter sur la baie de disques après la création de la réplique.
Voir aussi snapshot.

CRS

Processus (service) CRS (Cell Request Server ou serveur des requêtes de cellule) qui s'exécute sur le Gestionnaire de cellule Data Protector et lance et contrôle les sessions de sauvegarde et de restauration. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule. Sur les systèmes Windows, le CRS s'exécute sous le compte de l'utilisateur spécifié lors de l'installation. Sur les systèmes UNIX, il s'exécute sous le compte `root`.

cryptage AES 256 bits

Data Protector sur logiciel, basé sur l'algorithme de cryptage AES-CTR (Advanced Encryption Standard in Counter Mode) qui utilise des clés aléatoires d'une longueur de 256 bits. La même clé est utilisée à la fois pour le cryptage et le décryptage. Avec le cryptage AES 256 bits, les données sont cryptées avant d'être transférées sur un réseau et d'être écrites sur un support.

cryptage sur lecteur

Le cryptage sur lecteur Data Protector utilise la fonctionnalité de cryptage du lecteur. Lors de la sauvegarde, le lecteur crypte les données et les métadonnées qui sont écrites sur le support.

CSM

Le processus CSM Data Protector (Copy and Consolidation Session Manager - gestionnaire de session de copie et de consolidation) contrôle les sessions de copie et de consolidation d'objets et sexécute sur le système Gestionnaire de cellule.

Dbobject

(terme propre à Informix Server) Objet de base de données physique Informix Server. Il peut s'agir d'un blobspace, d'un dbspace ou d'un fichier journal logique.

DCBF

Les fichiers binaires de catalogue des détails (DCBF, pour Detail Catalog Binary Files), une partie de la base de données interne, contiennent les informations relatives aux attributs et aux versions de fichier. Ils occupent environ 80 % de l'espace de l'IDB. Un fichier binaire DC est créé par support Data Protector utilisé pour la sauvegarde. Sa taille maximale est limitée par les paramètres de système de fichiers.

délai d'expiration de la protection de données

Permet de définir le délai de protection des données sauvegardées sur un support, c'est-à-dire la durée pendant laquelle Data Protector ne peut les écraser. Une fois ce délai expiré, Data Protector peut réutiliser le support lors d'une prochaine session de sauvegarde.
Voir aussi protection de catalogue.

demande de montage

Message apparaissant à l'écran et invitant l'utilisateur à insérer un support spécifique dans un périphérique. Lorsque vous avez répondu à la demande de montage en fournissant le support requis et en confirmant, la session se poursuit.

dépôt de fichier

Fichier contenant les données d'une sauvegarde vers un périphérique de bibliothèque de fichiers.

disque auxiliaire

Disque amorçable possédant un système d'exploitation minimum avec réseau et Agent de disque Data Protector installé. Il peut être transporté et utilisé pour amorcer le système cible dans la première phase de la récupération après sinistre avec restitution de disque des clients UNIX.

disque virtuel

(terme propre à HP P6000 EVA Array Family) Unité de stockage allouée à partir d'un pool de stockage d'une baie de disques HP StorageWorks P6000 EVA Disk Array Family. Le disque virtuel est l'entité qui peut être répliquée à l'aide de la fonctionnalité Snapshot de la baie de disques.
Voir aussi volume source et volume cible.

disques partagés

Disque Windows situé sur un autre système et mis à la disposition d'autres utilisateurs sur le réseau.Les systèmes dotés de disques partagés peuvent être sauvegardés, même en l'absence d'un Agent de disque Data Protector.

DMZ

La zone démilitarisée (DMZ) est un réseau inséré en tant que "zone neutre" entre le réseau privé d'une société (intranet) et le réseau public extérieur (Internet). Elle empêche les utilisateurs externes d'accéder directement aux serveurs de la société sur l'intranet de celle-ci.

données sauvegardées publiques/privées

Lors de la configuration d'une sauvegarde, l'utilisateur peut indiquer si les données sauvegardées seront :

- publiques, c'est-à-dire visibles (et accessibles pour la restauration) par tous les utilisateurs de Data Protector

- privées, c'est-à-dire visibles (et accessibles pour la restauration) uniquement par le propriétaire de la sauvegarde et par les administrateurs.

données_programme_Data_Protector
Sous Windows Vista, Windows 7 et Windows Server 2008, il s'agit du répertoire contenant les fichiers de données Data Protector. Le chemin par défaut est `%ProgramData%\OmniBack`, mais vous pouvez le modifier dans l'assistant d'installation de Data Protector au moment de l'installation.
Voir aussi répertoire_Data_Protector.

DR OS
Environnement de système d'exploitation dans lequel la récupération après sinistre est effectuée. Il fournit à Data Protector un environnement d'exécution de base (accès au disque, au réseau, à la bande et au système de fichiers). Vous devez installer sur disque ou charger en mémoire et configurer le système d'exploitation avant d'exécuter la récupération après sinistre Data Protector. Le DR OS peut être temporaire ou actif. Un DR OS temporaire est exclusivement utilisé en tant qu'environnement hôte pour la restauration d'un autre système d'exploitation, conjointement avec les données de configuration du système d'exploitation cible. Il est supprimé à l'issue de la restauration du système cible dans la configuration système d'origine. Un DR OS actif héberge le processus de récupération après sinistre Data Protector et peut également faire partie du système restauré, car il remplace ses propres données de configuration par celles d'origine.

droits d'accès
Voir droits utilisateur.

droits utilisateur
Les droits utilisateur ou droits d'accès correspondent aux autorisations nécessaires pour exécuter certaines tâches dans Data Protector, telles que la configuration d'une sauvegarde, le démarrage d'une session de sauvegarde ou le lancement d'une session de restauration. Les utilisateurs disposent des droits d'accès du groupe d'utilisateurs auquel ils appartiennent.

échangeur
Egalement appelé échangeur SCSI.
Voir aussi bibliothèque.

emplacement
Position mécanique au sein d'une bibliothèque. Chaque emplacement peut contenir un support, comme une bande DLT. Data Protector attribue un numéro à chaque emplacement. Pour

être lu, un support est déplacé par un mécanisme robotique de son emplacement dans le lecteur.

emplacement d'un support Emplacement physique d'un support défini par l'utilisateur, par exemple, "bâtiment 4" ou "stockage hors site".

enregistrement circulaire *(terme propre à Microsoft Exchange Server et Lotus Domino Server)* L'enregistrement circulaire est un mode de base de données Microsoft Exchange Server et Lotus Domino Server dans lequel le contenu des fichiers journaux de transactions est périodiquement réécrit une fois que les données correspondantes ont été transmises à la base de données. L'enregistrement circulaire réduit les besoins en espace disque.

environnement de sauvegarde d'entreprise Plusieurs cellules peuvent être regroupées et gérées depuis une cellule centrale. L'environnement de sauvegarde d'entreprise comprend tous les clients répartis entre plusieurs cellules Data Protector, lesquelles sont gérées et administrées à partir d'une cellule centrale utilisant le concept Manager-of-Managers. *Voir aussi* MoM.

espace de table Partie de la structure d'une base de données. Chaque base de données est divisée de manière logique en un ou plusieurs espaces de table. Chaque espace de table contient des fichiers de données ou des volumes bruts qui lui sont exclusivement associés.

établissement (rétablissement) incrémental *(terme propre à EMC Symmetrix)* Opération de contrôle BCV ou SRDF. Dans les opérations de contrôle BCV, un établissement incrémental entraîne la synchronisation incrémentale du périphérique BCV et son fonctionnement en tant que support en miroir EMC Symmetrix. Des paires doivent avoir été préalablement définies entre les périphériques EMC Symmetrix. Dans les opérations de contrôle SRDF, un établissement incrémental entraîne la synchronisation incrémentale du périphérique (R2) cible et son fonctionnement en tant que support en miroir EMC Symmetrix. Des paires doivent avoir été préalablement définies entre les périphériques EMC Symmetrix.

état de paire *(terme propre à HP P9000 XP Array Family)* Etat dune paire de disques (volume secondaire et volume principal correspondant) dune baie de disques HP StorageWorks P9000 XP Disk Array Family. Selon les circonstances, les disques en paire peuvent se trouver dans divers états. Les états suivants sont

particulièrement importants pour le fonctionnement de l'Agent HP StorageWorks P9000 XP Data Protector :

- PAIRE – Le volume secondaire est préparé pour la sauvegarde avec temps d'indisponibilité nul. s'il s'agit d'un miroir, il est complètement synchronisé et s'il s'agit d'un volume à utiliser pour le stockage des snapshots, il est vide.
- SUSPENDU – Le lien entre les disques est suspendu. Toutefois, la relation de paire est maintenue et le disque secondaire peut à nouveau être préparé pour la sauvegarde avec temps d'indisponibilité nul.
- COPIE – La paire de disques est occupée et en cours de transition vers létat PAIRE. Si le volume secondaire est un miroir, il est resynchronisé avec le volume principal, et s'il s'agit d'un volume à utiliser pour le stockage des snapshots, son contenu est effacé.

état des supports Qualité des supports telle qu'elle est reflétée par les facteurs d'état des supports. Plus l'âge et l'utilisation faite des supports sont importants, plus les risques d'erreurs de lecture et d'écriture sont élevés sur les supports à bande. Un support doit être remplacé lorsque son état est MEDIOCRE.

état système *(terme propre à Windows)* Les données d'état système comprennent le registre, la base de données d'enregistrement de classe COM+, les fichiers de démarrage système et la base de données de services de certificats (à condition que le serveur soit du type "certificate server"). Si le serveur correspond à un contrôleur de domaine, les données d'état du système contiennent également les services Active Directory et le répertoire SYSVOL. Si le serveur exécute le service de cluster, les données d'état du système indiquent, par ailleurs, les points de contrôle du registre des ressources et le journal de récupération de ressource quorum, qui contient les informations à jour sur la base de données des clusters.

étiquette de support Identificateur défini par l'utilisateur et servant à décrire un support.

exécution multisnap *(terme propre à HP P6000 EVA Array Family)* Création simultanée de volumes cibles pour assurer la cohérence des données de sauvegarde sur chacun des volumes cibles, mais aussi sur tous les volumes constituant un snapshot.
Voir aussi snapshot.

exportation de supports

Procédé consistant à supprimer de la base de données IDB toutes les données relatives aux sessions de sauvegarde (comme les systèmes, objets et noms des fichiers qui résident sur le support). Les informations relatives aux supports et à leur relation par rapport à un pool sont également supprimées de la base de données IDB. Toutefois, les données enregistrées sur les supports restent inchangées.
Voir aussi importation de supports.

facteurs d'état des supports

Limites d'âge et de réécriture définies par l'utilisateur pour déterminer l'état d'un support.

Fibre Channel

Norme ANSI pour l'interconnexion informatique à haute vitesse. Utilisant des câbles à fibre optique ou en cuivre, cette technologie permet la transmission bidirectionnelle ultra-rapide de fichiers de données volumineux, et peut être déployée entre des sites distants de plusieurs kilomètres. La technologie Fibre Channel relie les noeuds au moyen de trois topologies physiques différentes : point à point, en boucle et par commutation.

fichier CDF

(terme propre à UNIX) Context Dependent File, fichier contextuel - Il s'agit d'un fichier constitué de plusieurs fichiers regroupés sous le même chemin d'accès. Le système sélectionne habituellement l'un des fichiers à l'aide du contexte du processus. Ce mécanisme permet à des exécutables dépendant des machines, à des fichiers de données système et à des fichiers de périphériques de fonctionner correctement depuis l'ensemble des hôtes d'un cluster, tout en utilisant le même chemin d'accès.

fichier d'amorçage d'urgence

(terme propre à Informix Server) Fichier de configuration Informix Server `ixbar.server_id` qui réside dans le répertoire `INFORMIXDIR/etc` (sous Windows) ou `INFORMIXDIR\etc` (sous UNIX). `INFORMIXDIR` est le répertoire de base d'Informix Server et `ID_serveur` la valeur du paramètre de configuration `SERVERNUM`. Chaque ligne du fichier d'amorçage d'urgence correspond à un objet sauvegarde.

fichier d'options globales

Fichier permettant à l'utilisateur de personnaliser Data Protector. Ce fichier fournit des informations sur les options globales, lesquelles concernent différents aspects de Data Protector, généralement les délais d'attente et les limites, et affectent la cellule Data Protector entière. Le fichier se trouve sur le Gestionnaire de cellule dans le répertoire

données_programme_Data_Protector\Config\Server\Options (Windows Server 2008), `répertoire_Data_Protector\Config\Server\Options` (autres systèmes Windows) ou `/etc/opt/omni/server/options` (systèmes HP-UX, Solaris et Linux).

fichier de contrôle *(terme propre à Oracle et SAP R/3)* Fichier de données Oracle contenant des entrées spécifiant la structure physique de la base de données. Il fournit des informations sur la cohérence de la base de données utilisées pour la récupération.

fichier de données *(terme propre à Oracle et SAP R/3)* Fichier physique créé par Oracle et contenant des structures de données telles que les tables et index. Un fichier de données ne peut appartenir qu'à une seule base de données Oracle.

fichier de données de récupération système *Voir* fichier DRS.

fichier de récupération de l'IDB Fichier IDB (obrindex.dat) contenant des informations sur les sauvegardes IDB, les périphériques et les supports utilisés pour la sauvegarde. Ces données peuvent simplifier considérablement la récupération de la base de données IDB. Il est recommandé de déplacer le fichier et les journaux de transactions de l'IDB sur un disque physique séparé des autres répertoires de l'IDB, mais aussi de créer une autre copie du fichier.

fichier DRS *(terme propre à la récupération après sinistre)* Ficher texte au format Unicode (UTF-16), généré au cours de la sauvegarde de la CONFIGURATION d'un système Windows ou Linux et stocké sur le Gestionnaire de cellule. Il contient les informations système requises pour installer et configurer le système d'exploitation sur le système cible en cas de sinistre.
Voir aussi système cible.

fichier épars Fichier contenant des données avec des parties de bloc vides. Exemples : matrice dont une partie ou la plupart des données contient des zéros, fichiers provenant d'applications de visualisation d'images, bases de données rapides. Si l'option de traitement des fichiers épars n'est pas activée pendant la restauration, cette opération peut s'avérer impossible.

fichier Jours chômés

Fichier contenant des informations sur les jours chômés. Vous pouvez définir des jours chômés différents en modifiant le fichier Jours chômés sur le Gestionnaire de cellule, dans le répertoire données_programme_Data_Protector\Config\Server\holidays (Windows Server 2008), `répertoire_Data_Protector\Config\Server\holidays` (autres systèmes Windows) ou `/etc/opt/omni/server/Holidays` (systèmes UNIX).

fichier P1S

Fichier `P1S` contenant des informations sur le formatage et le partitionnement de tous les disques installés sur un système lors d'une récupération après sinistre automatisée évoluée (EADR). Créé durant la sauvegarde complète, il est enregistré sur un support de sauvegarde et sur le Gestionnaire de cellule dans le répertoire `données_programme_Data_Protector\Config\Server\dr\p1s` (Windows Server 2008), `répertoire_Data_Protector\Config\Server\dr\p1s` (autres systèmes Windows) ou `/etc/opt/omni/server/dr/p1s` (systèmes UNIX), sous le nom `recovery.p1s`.

fichier sqlhosts ou registre

(terme propre à Informix Server) Registre (sous Windows) ou fichier d'informations de connectivité Informix Server (sous UNIX) contenant les noms de tous les serveurs de base de données, ainsi que tous les alias auxquels les clients d'un ordinateur hôte peuvent se connecter.

fichier sst.conf

Le fichier `/usr/kernel/drv/sst.conf` doit être présent sur chaque client Sun Solaris Data Protector auquel un périphérique de bibliothèque multi-lecteurs est connecté. Il doit contenir une entrée pour l'adresse SCSI du mécanisme robotique de chaque périphérique de bibliothèque connecté au client.

fichier st.conf

Le fichier `/kernel/drv/st.conf` doit être présent sur chaque client Solaris Data Protector auquel un périphérique de sauvegarde est connecté. Il doit contenir des informations sur le périphérique et une adresse SCSI pour chaque lecteur de sauvegarde connecté au client. Une seule entrée SCSI est requise pour un périphérique à lecteur unique, tandis qu'il en faut plusieurs pour un périphérique de bibliothèque multi-lecteurs.

fichier TSANDS.CFG

(terme propre à Novell NetWare) Fichier permettant à l'utilisateur de spécifier les noms des conteneurs à partir desquels les sauvegardes doivent commencer. Il s'agit d'un fichier texte

situé dans le répertoire SYS:SYSTEM\TSA du serveur où est chargé TSANDS.NLM.

fichier user_restrictions

Fichier qui restreint certaines opérations, disponibles pour le groupe d'utilisateurs Data Protector en fonction des droits utilisateur affectés, que les utilisateurs peuvent effectuer sur des systèmes spécifiques de la cellule Data Protector. Ces restrictions s'appliquent uniquement aux groupes d'utilisateurs Data Protector autres que *Administrateur* et *Opérateur*.

fichiers de journal des transactions

Il s'agit des fichiers dans lesquels sont enregistrées les modifications de base de données. Ils assurent également une fonction de tolérance aux pannes en cas de sinistre au niveau d'une base de données.

fichiers de récupération

(terme propre à Oracle) Les fichiers de récupération sont des fichiers propres à Oracle qui résident dans la zone de récupération flash : fichier de contrôle actuel, journaux de rétablissement en ligne, journaux de rétablissement archivés, journaux de flashback, sauvegardes automatiques de fichier de contrôle, copies de fichier de données et éléments de sauvegarde.
Voir aussi zone de récupération flash.

fichiers journaux logiques

Concerne la sauvegarde de base de données en ligne. Les fichiers journaux logiques sont des fichiers dans lesquels les données modifiées sont stockées avant d'être transférées au disque. En cas de panne, les fichiers journaux logiques permettent d'implémenter toutes les transactions qui ont été transférées et d'annuler toutes celles qui ne l'ont pas encore été.

flux de données

Séquence de données transférées via le canal de communication.

fnames.dat

Les fichiers fnames.dat de la base de données IDB contiennent des informations sur les noms des fichiers sauvegardés. Ces fichiers occupent généralement 20 % environ de la base de données IDB si des noms de fichiers sont stockés.

format de support de fichiers distribués

Format de support, disponible avec la bibliothèque de fichiers, qui prend en charge un type de sauvegarde synthétique très économe en espace disque, appelée "sauvegarde complète

virtuelle". L'utilisation de ce format est une condition préalable à la sauvegarde complète virtuelle.
Voir aussi sauvegarde complète virtuelle.

formatage

Processus consistant à effacer toutes les données contenues sur un support et à préparer ce dernier pour l'utiliser avec Data Protector. Les informations relatives au support (ID du support, description et emplacement) sont enregistrées dans la base IDB ainsi que sur les supports concernés (en en-tête de ces derniers). Les supports Data Protector comportant des données protégées ne sont pas formatés tant que la protection n'a pas expiré ou que la protection du support n'est pas retirée ou le support recyclé.

fournisseur de copie miroir

(terme propre à Microsoft VSS) Entité réalisant la création et la représentation des copies miroir des volumes. Les fournisseurs possèdent les données des copies miroir et exposent les copies miroir. Ces fournisseurs peuvent être de type logiciel (fournisseurs système, par exemple) ou matériel (disques locaux, baies de disques).
Voir aussi copie miroir.

fusion

La fusion correspond à un mode de résolution de conflit de fichiers au cours d'une restauration. Si le fichier à restaurer se trouve déjà à l'emplacement de destination, c'est celui dont la date de modification est la plus récente qui est conservé. Les fichiers qui ne sont pas présents sur le disque sont toujours restaurés.
Voir aussi réécriture.

Fournisseur HP StorageWorks SMI-S P6000 EVA Array

Interface permettant de contrôler HP StorageWorks P6000 EVA Disk Array Family. Le fournisseur SMI-S P6000 EVA Array s'exécute en tant que service distinct sur le système de gestion du stockage HP et agit comme passerelle entre les requêtes entrantes et HP StorageWorks Command View EVA. Grâce à l'intégration de Data Protector avec HP P6000 EVA Array Family, le fournisseur SMI-S P6000 EVA Array accepte les requêtes standardisées de l'Agent P6000 EVA SMI-S, communique avec HP StorageWorks Command View EVA pour l'appel d'informations ou de méthodes et renvoie des réponses standardisées.
Voir aussi Agent HP StorageWorks P6000 EVA SMI-S et HP StorageWorks Command View (CV) EVA.

génération de rapports Web

Fonction Data Protector permettant à l'utilisateur d'afficher des rapports sur l'état de la sauvegarde, de la consolidation et de la copie d'objet, ainsi que sur la configuration Data Protector à l'aide de l'interface Web.

génération de sauvegarde

Une génération de sauvegarde est constituée d'une sauvegarde complète, ainsi que de toutes les sauvegardes incrémentales effectuées jusqu'à la prochaine sauvegarde complète.

gestion centralisée des licences

Data Protector permet de configurer une gestion centralisée des licences pour l'ensemble de l'environnement de l'entreprise, constitué de plusieurs cellules. Toutes les licences Data Protector sont installées et conservées dans le système du Gestionnaire de cellule d'entreprise. En fonction de vos besoins, vous pouvez ensuite affecter des licences à des cellules spécifiques.
Voir aussi MoM.

gestion de stockage automatique (ASM)

(terme propre à Oracle) Gestionnaire de systèmes de fichiers et de volumes intégré à Oracle qui gère les fichiers de base de données Oracle. Il simplifie la gestion des données et des disques et optimise les performances en fournissant des fonctions de mise en miroir et de répartition sur plusieurs axes.

Gestion de stockage hiérarchique (HSM, pour Hierarchical Storage Management)

Méthode visant à optimiser l'utilisation de l'espace disque pour le stockage des données et consistant à faire migrer les données les moins souvent utilisées vers des disques optiques moins coûteux. Lorsque cela est nécessaire, les données migrent de nouveau sur le disque dur. Cette méthode permet de trouver un équilibre entre le besoin d'extraire rapidement les données du disque dur et l'utilisation de disques optiques moins coûteux.

Gestionnaire de cellule

Système principal de la cellule dans lequel est installé le logiciel Data Protector central et d'où sont gérées toutes les activités de sauvegarde et de restauration. L'interface graphique utilisée pour les opérations de gestion peut se trouver sur un système différent. Chaque cellule dispose d'un système de Gestionnaire de cellule.

Gestionnaire de clés

(terme propre à Microsoft Exchange Server) Service Microsoft Exchange Server qui fournit une fonction de cryptage pour une meilleure sécurité.
Voir aussi banque d'informations et service de réplication de sites.

gestionnaire de récupération (RMAN)

(terme propre à Oracle) Interface de ligne de commande Oracle contrôlant un processus du serveur Oracle pour la sauvegarde, la restauration ou la récupération de la base de données à laquelle il est connecté. RMAN stocke les informations sur les sauvegardes dans le catalogue de récupération ou dans le fichier de contrôle. Ces informations peuvent être utilisées lors de sessions de restauration ultérieures.

Gestionnaire RAID P9000 XP (RM)

(terme propre à HP P9000 XP Array Family) L'application Gestionnaire RAID P9000 XP fournit une liste complète de commandes permettant de signaler et de contrôler l'état des applications HP CA P9000 XP et HP BC P9000 XP. Ces commandes communiquent avec l'unité de commande de disque HP StorageWorks P9000 XP Disk Array Family par le biais d'une instance du Gestionnaire RAID P9000 XP. Cette instance convertit les commandes en une séquence de commandes SCSI de bas niveau.

groupe

(terme propre à Microsoft Cluster Server) Ensemble de ressources (par exemple, des volumes de disque, des services d'applications, des noms et adresses IP) nécessaires à l'exécution d'applications compatibles cluster spécifiques.

groupe d'utilisateurs

Chaque utilisateur de Data Protector est membre d'un groupe d'utilisateurs, Et chaque utilisateur faisant partie d'un groupe d'utilisateurs reçoit les mêmes droits. Le nombre de groupes d'utilisateurs et leurs droits utilisateur peuvent être définis librement. Dans Data Protector, on distingue trois groupes d'utilisateurs par défaut : Admin, Opérateur et Utilisateur.

groupe de disques

(terme propre à Veritas Volume Manager) Unité de base de stockage des données dans un système VxVM. Un groupe de disques peut être constitué d'un ou de plusieurs volumes physiques. Le système peut contenir plusieurs groupes de disques.

groupe de périphériques

(terme propre à EMC Symmetrix) Unité logique représentant plusieurs périphériques EMC Symmetrix. Un même périphérique ne peut appartenir à plus d'un groupe de périphériques. Tous les périphériques d'un groupe doivent se trouver sur la même unité EMC Symmetrix. Les groupes de périphériques vous permettent d'identifier et d'utiliser un sous-ensemble de périphériques EMC Symmetrix disponibles.

groupe de réplication de données
(terme propre à HP P6000 EVA Array Family) Regroupement logique de disques virtuels HP P6000 EVA Array Family. Ce groupe peut contenir jusqu'à huit jeux de copies à condition qu'ils aient des caractéristiques communes et partagent un journal HP CA P6000 EVA commun.
Voir aussi jeu de copies.

groupe de stockage
(terme propre à Microsoft Exchange Server) Regroupement de banques de boîtes aux lettres et de dossiers publics se partageant un ensemble de fichiers journaux de transactions. Exchange Server gère chaque groupe de stockage au moyen d'un processus de serveur distinct.

groupe de volumes
Unité de stockage des données dans un système LVM. Un groupe de volumes peut être constitué d'un ou plusieurs volumes physiques. Le système peut contenir plusieurs groupes de volumes.

HP Business Copy (BC) P6000 EVA
(terme propre à HP P6000 EVA Array Family) Solution logicielle de réplication locale qui permet de créer des copies à un instant donné (répliques) des volumes sources en utilisant les fonctions de snapshot et de clonage du microprogramme P6000 EVA.
Voir aussi réplique, volume source, snapshot et HP Continuous Access + Business Copy (CA + BC) P6000 EVA.

HP Business Copy (BC) P9000 XP
(terme propre à HP P9000 XP Array Family) Configuration HP StorageWorks P9000 XP Disk Array Family qui permet de créer et de gérer des copies internes de LDEV à des fins aussi diverses que la sauvegarde et la duplication de données. Les copies (volumes secondaires ou S-VOL) peuvent être séparées des volumes principaux (P-VOL) et connectées à un système différent. Pour la sauvegarde avec temps d'indisponibilité nul Data Protector, les P-VOL doivent être disponibles pour le système d'application et l'un des jeux de miroirs S-VOL doit être disponible pour le système de sauvegarde.
Voir aussi LDEV , HP Continuous Access (CA) P9000 XP, unité de commande principale, système d'application et système de sauvegarde.

HP Continuous Access (CA) P9000 XP
(terme propre à HP P9000 XP Array Family) Configuration HP StorageWorks P9000 XP Disk Array Family qui permet de créer et de gérer des copies distantes de LDEV à des fins aussi diverses que la sauvegarde, la duplication de données et la récupération après sinistre. Les opérations HP CA P9000 XP impliquent les

baies de disques principales et distantes (secondaires). Les premières sont connectées au système dapplication et contiennent les volumes principaux (P-VOL) sur lesquels les données dorigine sont stockées. Les baies de disques secondaires sont connectées au système de sauvegarde et contiennent les volumes secondaires (S-VOL).
Voir aussi HP Business Copy (BC) P9000 XP, unité de commande principale et LDEV.

HP Continuous Access + Business Copy (CA + BC) P6000 EVA

(terme propre à HP P6000 EVA Array Family) Configuration HP StorageWorks P6000 EVA Disk Array Family qui permet de créer et de gérer des copies (répliques) des volumes sources sur une baie P6000 EVA distante, puis d'utiliser ces copies comme source pour une réplication locale sur cette baie distante.
Voir aussi HP Business Copy (BC) P6000 EVA, réplique et volume source.

HP StorageWorks Command View (CV) EVA

(terme propre à HP P6000 EVA Array Family) Interface utilisateur permettant de configurer, de gérer et de surveiller le système de stockage P6000 EVA. Elle est utilisée pour effectuer diverses tâches de gestion du stockage, par exemple, la création de familles de disques virtuels, la gestion du matériel de stockage et la création de snapshots, de snapclones et de mirrorclones de disques virtuels. Le logiciel HP StorageWorks Command View EVA s'exécute sur le système de gestion du stockage HP. Il est accessible via un navigateur Web.
Voir aussi Agent HP StorageWorks P6000 EVA SMI-S et fournisseur HP StorageWorks SMI-S P6000 EVA Array.

HP Operations Manager

HP Operations Manager offre des fonctions puissantes pour gérer les opérations d'un grand nombre de systèmes et d'applications à l'intérieur d'un réseau. Data Protector fournit une intégration de ce produit de gestion. Cette intégration est mise en œuvre sous la forme d'un module SMART Plug-In pour les serveurs de gestion HP Operations Manager sous Windows, HP-UX, Solaris et Linux. Les versions antérieures de HP Operations Manager se nommaient IT/Operation, Operations Center, Vantage Point Operations et Openview Operations.

HP Operations Manager SMART Plug-In (SPI)

Solution entièrement intégrée et prête à l'emploi qui vient compléter HP Operations Manager, élargissant ainsi le domaine géré. Grâce à l'intégration Data Protector, mise en oeuvre sous la forme d'un module HP Operations Manager SMART Plug-In,

un utilisateur peut mettre en place la surveillance d'un nombre arbitraire de Gestionnaires de cellule Data Protector en tant qu'extension de HP Operations Manager.

ICDA *(terme propre à EMC Symmetrix)* ICDA (Integrated Cached Disk Arrays) d'EMC est un périphérique à baie de disques combinant un ensemble de disques physiques, un certain nombre de canaux FWD SCSI, une mémoire cache interne et un logiciel de contrôle et de diagnostic communément appelé "microcode".

ID clé de cryptage-ID Banque Identificateur combiné utilisé par le serveur gestionnaire de clés Data Protector pour identifier et administrer les clés de cryptage utilisées par Data Protector. `IDClé` identifie la clé dans la banque de clés. `IDBanque` identifie la banque de clés dans le Gestionnaire de cellule. Si Data Protector a été mis à niveau à partir d'une version précédente avec la fonctionnalité de cryptage, il se peut que plusieurs `IDBanque` soient utilisés sur le même Gestionnaire de cellule.

ID d'objet *(terme propre à Windows)* Les ID d'objet (OID) permettent d'accéder aux fichiers NTFS 5, quel que soit l'emplacement de ces derniers au sein du système. Data Protector considère les OID comme des flux de fichiers.

ID de connexion *(terme propre à Microsoft SQL Server)* Nom sous lequel un utilisateur se connecte à Microsoft SQL Server. Pour qu'un ID de connexion soit reconnu, une entrée doit avoir été créée pour l'utilisateur auquel il appartient dans la table système syslogin de Microsoft SQL Server.

ID de sauvegarde L'identificateur d'un objet d'intégration qui est similaire à l'ID de session de la sauvegarde de l'objet en question. L'ID de sauvegarde est conservé lorsque l'objet est copié, exporté ou importé.

ID de session Identificateur d'une session de sauvegarde, de restauration, de copie d'objet, de consolidation d'objet, de vérification d'objet ou de gestion de supports, qui est constitué de la date d'exécution de la session et d'un numéro unique.

ID de support de données Identificateur unique attribué à un support par Data Protector.

IDB

Base de données interne de Data Protector. Il s'agit d'une base de données intégrée résidant sur le Gestionnaire de cellule. Elle contient des informations sur les données sauvegardées, sur les supports utilisés pour la sauvegarde, sur les modalités d'exécution des sessions de sauvegarde, de restauration, etc., ainsi que sur les périphériques, bibliothèques et baies de disques configurés.

image DR

Données nécessaires à l'installation et la configuration du système d'exploitation temporaire de récupération après sinistre (DR OS).

importation de supports

Procédé consistant à relire dans la base de données IDB l'ensemble des données relatives aux sessions de sauvegarde qui se trouvent sur le support. Ceci permet ensuite à l'utilisateur d'accéder rapidement et facilement aux données stockées sur les supports.
Voir aussi exportation de supports.

index de lecteur

Numéro permettant d'identifier la position mécanique d'un lecteur au sein d'une bibliothèque. Le contrôle robotique utilise ce numéro pour accéder à un lecteur.

Inet

Processus s'exécutant sur chaque système UNIX ou service s'exécutant sur chaque système Windows dans la cellule Data Protector. Il est responsable de la communication entre les systèmes de la cellule et du lancement des processus requis pour la sauvegarde et la restauration. Le service Inet est lancé dès que Data Protector est installé sur un système. Le processus Inet est démarré par le démon inetd.

informations d'audit

Données concernant chaque session de sauvegarde effectuée sur une période étendue et définie par l'utilisateur, sur l'ensemble de la cellule Data Protector.

informations de connexion à la base de données cible Oracle

(terme propre à Oracle et SAP R/3) Le format des informations de connexion est le suivant :
`nom_utilisateur/mot_de_passe@service`, où :

- `nom_utilisateur` est le nom sous lequel un utilisateur est reconnu par le serveur Oracle et par les autres utilisateurs. Chaque nom d'utilisateur est associé à un mot de passe ; l'utilisateur doit les entrer tous les deux pour pouvoir se connecter à une base de données cible Oracle. Il doit également disposer de droits SYSDBA ou SYSOPER Oracle.

- *mot_de_passe* doit correspondre à celui figurant dans le fichier de mots de passe Oracle (orapwd) ; ce fichier permet d'authentifier les utilisateurs chargés de l'administration de la base de données.
- *service* est le nom servant à identifier un processus du serveur SQL*Net pour la base de données cible.

informations de connexion à la base de données du catalogue de récupération

(terme propre à Oracle) Le format des informations de connexion à la base de données du catalogue de récupération (Oracle) est le suivant : *nom_utilisateur/mot de passe@service*, où la description du nom d'utilisateur, du mot de passe et du nom du service est la même que celle qui figure dans les informations de connexion SQL*Net V2 à la base de données cible Oracle. Dans ce cas, le *service* correspond au nom du service de la base de données catalogue de récupération et non à la base de données cible Oracle. Notez que l'utilisateur Oracle spécifié doit être le propriétaire du catalogue de récupération Oracle.

Informix Server

(terme propre à Informix Server) Fait référence à Informix Dynamic Server.

initialisation

Voir formatage.

instance Oracle

(terme propre à Oracle) Chaque installation d'une base de données Oracle sur un ou plusieurs systèmes. Plusieurs instances de base de données peuvent s'exécuter sur un même système informatique.

interface de ligne de commande (CLI)

Ensemble de commandes de type DOS et UNIX qui peuvent être utilisées dans les scripts shell pour effectuer des tâches de configuration, de sauvegarde, de restauration et de gestion.

interface de périphérique virtuel

(terme propre à Microsoft SQL Server) Interface de programmation de SQL Server permettant de sauvegarder et de restaurer rapidement des bases de données volumineuses.

Interface utilisateur graphique (GUI)

Interface utilisateur graphique fournie par Data Protector pour offrir un accès aisé à l'ensemble des tâches de configuration, d'administration et d'utilisation. En plus de son interface utilisateur graphique d'origine sous Windows, Data Protector fournit également une interface Java d'apparence et de fonctionnalités similaires pour bon nombre d'autres plates-formes.

interface XBSA

(terme propre à Informix Server) L'utilitaire ON-Bar et Data Protector communiquent par le biais de l'interface de programmation XBSA (X/Open Backup Services Application).

Internet Information Services (IIS)

(terme propre à Windows) Microsoft Internet Information Services est un serveur d'applications et de fichiers réseau qui prend en charge de nombreux protocoles. La fonction principale d'IIS consiste à transmettre les informations des pages HTML (Hypertext Markup Language) à l'aide du protocole HTTP (Hypertext Transport Protocol).

ISQL

(terme propre à Sybase) Utilitaire Sybase utilisé pour exécuter des tâches d'administration système sur Sybase SQL Server.

Jeu ASR

Ensemble de fichiers stockés sur plusieurs disquettes, nécessaires pour la reconfiguration appropriée du disque de rechange (partition du disque et configuration des volumes logiques), ainsi que pour la récupération automatique du système d'origine et des données utilisateur sauvegardées lors de la sauvegarde complète du client. Ces fichiers sont stockés comme fichier archive ASR sur le Gestionnaire de cellule dans le répertoire `données_programme_Data_Protector\Config\Server\dr\asr` (Windows Server 2008), `répertoire_Data_Protector\Config\Server\dr\asr` (autres systèmes Windows) ou `/etc/opt/omni/server/dr/asr` (systèmes UNIX) ainsi que sur le support de sauvegarde. Après un sinistre, le fichier archive ASR est extrait sur des disquettes dont vous aurez besoin pour exécuter le processus de récupération automatique du système.

jeu de copies

(terme propre à HP P6000 EVA Array Family) Paire constituée des volumes sources sur une baie P6000 EVA locale et de leur réplique sur une baie P6000 EVA distante.
Voir aussi volume source, réplique et HP Continuous Access + Business Copy (CA + BC) P6000 EVA

jeu de copies miroir

(terme propre à Microsoft VSS) Ensemble de copies miroir créées au même instant.
Voir aussi copie miroir et jeu de répliques.

jeu de répliques

(terme propre à ZDB) Groupe de répliques, toutes créées en utilisant la même spécification de sauvegarde.
Voir aussi réplique et rotation des jeux de répliques.

jeu de sauvegarde Jeu complet d'objets d'intégration associés à une sauvegarde.

jeu de sauvegarde *(terme propre à Oracle)* Regroupement logique de fichiers sauvegardés créés à l'aide de la commande de sauvegarde RMAN. Un jeu de sauvegarde est un ensemble complet de fichiers associés à une sauvegarde. Pour améliorer les performances, les fichiers peuvent être multiplexés. Un jeu de sauvegarde contient des fichiers de données ou des journaux d'archive, mais pas les deux à la fois.

jeu de supports Une session de sauvegarde a pour résultat le stockage de données sur un groupe de supports appelé "jeu de supports". Selon la stratégie d'utilisation des supports, plusieurs sessions peuvent se partager les mêmes supports.

jonction de répertoire *(terme propre à Windows)* Les jonctions de répertoires utilisent le concept de point d'analyse de Windows. Une jonction de répertoire NTFS 5 permet à l'utilisateur de rediriger une requête de répertoire/fichier vers un autre emplacement.

journal d'événements (journal d'événements Data Protector) Référentiel central de l'ensemble des notifications ayant trait à Data Protector. Par défaut, toutes les notifications sont envoyées au journal d'événements. Les événements sont consignés sur le Gestionnaire de cellule dans le fichier `données_programme_Data_Protector\log\server\Ob2EventLog.txt` (Windows Server 2008), `répertoire_Data_Protector\log\server\Ob2EventLog.txt` (autres systèmes Windows) ou `/var/opt/omni/server/log/Ob2EventLog.txt` (systèmes UNIX). Le journal d'événements n'est accessible qu'aux utilisateurs appartenant au groupe `Admin` de Data Protector et à ceux qui disposent des droits utilisateur `Rapports et notifications` Data Protector. Vous pouvez afficher ou supprimer l'ensemble des événements du journal.

journal de rétablissement *(terme propre à Oracle)* Chaque base de données Oracle dispose d'un ensemble de plusieurs fichiers journaux de rétablissement. Cet ensemble est appelé "journal de rétablissement de la base de données". Oracle y consigne toutes les modifications apportées aux données.

journal de rétablissement archivé *(terme propre à Oracle)* Egalement appelé journal de rétablissement hors ligne. Si la base de données Oracle fonctionne en mode ARCHIVELOG, chaque journal de

rétablissement en ligne, lorsqu'il est plein, est copié dans un emplacement de destination des journaux archivés. Cette copie est appelée journal de rétablissement archivé. La présence ou l'absence d'un journal de rétablissement archivé est déterminée par le mode que la base de données utilise :

- ARCHIVELOG - Les fichiers journaux de rétablissement en ligne pleins sont archivés avant d'être réutilisés. La base de données peut être récupérée en cas de défaillance d'un disque ou d'une instance. Vous ne pouvez effectuer de sauvegarde "à chaud" que si la base de données fonctionne dans ce mode.
- NOARCHIVELOG - Les fichiers journaux de rétablissement en ligne ne sont pas archivés.

Voir aussi journal de rétablissement en ligne.

journal de rétablissement en ligne

Voir journal de rétablissement archivé.

journal de rétablissement en ligne

(terme propre à Oracle) Journaux de rétablissement qui n'ont pas été archivés, mais qui sont à la disposition de l'instance à des fins d'enregistrement de la base de données ou qui sont pleins et attendent d'être archivés ou réutilisés.
Voir aussi journal de rétablissement archivé.

Journal des modifications

(terme propre à Windows) Fonction du système de fichiers Windows, qui consigne un enregistrement de chaque modification survenant au niveau des fichiers et répertoires d'un volume NTFS local.

journaux d'audit

Fichiers de données dans lesquels les informations d'audit sont stockées.

journaux d'événements

(terme propre à Windows) Fichiers dans lesquels Windows consigne tous les événements, tels que le démarrage ou l'arrêt des services et les connexions et déconnexions des utilisateurs. Data Protector peut sauvegarder les journaux d'événements Windows dans le cadre de la sauvegarde de la configuration Windows.

journaux de transactions

(terme propre à Data Protector) Assure le suivi des modifications de la base de données IDB. Il est recommandé d'activer l'archivage des journaux de transactions pour éviter de perdre

les fichiers journaux créés après la dernière sauvegarde de l'IDB et nécessaires à sa récupération.

keychain Outil évitant d'avoir à fournir manuellement une phrase passe pour décrypter la clé privée. Vous devez l'installer et le configurer sur le Serveur d'installation si vous exécutez une installation à distance via un shell sécurisé.

KMS Le serveur gestionnaire de clés (KMS - Key Management Server) est un service centralisé qui s'exécute sur le Gestionnaire de cellule et assure la gestion des clés pour la fonctionnalité de cryptage Data Protector. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.

LBO *(terme propre à EMC Symmetrix)* Un objet sauvegarde logique (LBO, pour Logical Backup Object) est un objet de stockage/récupération de données dans l'environnement EMC Symmetrix. Il est stocké/récupéré par EMC Symmetrix comme une entité unique et ne peut être restauré que dans son intégralité.

LCR (local continuous replication) *(terme propre à Microsoft Exchange Server)* La réplication continue locale (LCR, pour Local Continuous Replication) est une solution sur serveur unique, qui crée et conserve une copie exacte (copie LCR) d'un groupe de stockage. Une copie LCR réside sur le même serveur que le groupe de stockage d'origine. Suite à sa création, une copie LCR est maintenue à jour par le biais de la technologie de propagation des modifications (réexécution des journaux). La fonction de réplication de LCR garantit que les journaux qui n'ont pas été répliqués ne sont pas supprimés. En conséquence de ce fonctionnement, l'exécution de sauvegardes dans un mode qui supprime les journaux risque de ne pas libérer d'espace si la réplication est suffisamment loin derrière en matière de copie des journaux. Les copies LCR servent à des fins de récupération après sinistre, puisqu'il est possible de basculer sur la copie LCR en quelques secondes. Si une copie LCR servant à la sauvegarde est située sur un disque différent de celui des données d'origine, la charge des E/S sur une base de données de production s'avère alors minimale.
Un groupe de stockage répliqué est représenté en tant que nouvelle instance du module d'écriture Exchange nommé Service

de réplication Exchange et peut être sauvegardé (à l'aide de VSS) comme n'importe quel groupe de stockage.
Voir aussi Cluster Continuous Replication et service de réplication Exchange.

LDEV

(terme propre à HP P9000 XP Array Family) Partition logique d'un disque physique d'une baie de disques HP StorageWorks P9000 XP Disk Array Family. Le LDEV est l'entité qui peut être répliquée à l'aide de la fonctionnalité Split Mirror ou Snapshot de la baie de disques.
Voir aussi HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP et réplique.

lecteur

Unité physique recevant des données provenant d'un système informatique et capable de les écrire sur un support magnétique (généralement un lecteur de bande). Un lecteur peut également lire les données du support et les envoyer au système informatique.

liste de préallocation

Dans un pool de supports, sous-ensemble de supports définissant l'ordre dans lequel les supports sont utilisés pour la sauvegarde.

LISTENER.ORA

(terme propre à Oracle) Fichier de configuration Oracle décrivant un ou plusieurs listeners TNS (Transparent Network Substrate) sur un serveur.

make_net_recovery

`make_net_recovery` est une commande Ignite-UX qui permet de créer une archive de récupération via le réseau sur le serveur Ignite-UX ou tout autre système spécifié. Le système cible peut être récupéré via les sous-réseaux après démarrage à l'aide d'une bande amorçable créée par la commande Ignite-UX `make_boot_tape` ou lorsque le système démarre directement à partir du serveur Ignite-UX. Vous pouvez automatiser le démarrage direct via le serveur Ignite-UX à l'aide de la commande Ignite-UX `bootsys` ou le spécifier en mode interactif sur la console d'amorçage.

make_tape_recovery

`make_tape_recovery` est une commande Ignite-UX qui permet de créer une bande (d'installation) de récupération amorçable adaptée au système et de mettre en oeuvre la récupération après sinistre sans surveillance en connectant le périphérique de sauvegarde directement au système cible et en démarrant le système cible à partir de la bande de récupération amorçable.

Le périphérique de sauvegarde doit être connecté au client en local durant la création des archives et la récupération du client.

Manager-of-Managers (MoM) *Voir* MoM.

MAPI *(terme propre à Microsoft Exchange server)* L'interface MAPI (Messaging Application Programming Interface) est l'interface de programmation qui permet aux applications et aux clients de messagerie de communiquer avec les systèmes de messagerie et d'information.

MCU *Voir* unité de commande principale (MCU, pour Main Control Unit).

Microsoft Exchange Server Système de messagerie "client-serveur" et de groupes de travail fournissant une connexion transparente à de nombreux systèmes de communication différents. Il offre aux utilisateurs un système de messagerie électronique, une solution de planification de groupe et individuelle, des formulaires en ligne et des outils d'automatisation du flux de travail. Il fournit également au développeur une plate-forme sur laquelle il peut élaborer des applications personnalisées de partage d'informations et de service de messagerie.

Microsoft Management Console (MMC) *(terme propre à Windows)* Modèle d'administration pour environnements Windows. Cette console met à votre disposition une interface utilisateur d'administration simple, cohérente et intégrée permettant de gérer de nombreuses applications à partir d'une seule et même interface, à condition toutefois que les applications soient compatibles avec le modèle MMC.

Microsoft SQL Server Système de gestion de base de données destiné à répondre aux besoins du traitement distribué "client-serveur".

Microsoft Volume Shadow Copy Service (VSS) Service logiciel offrant une interface de communication unifiée destinée à coordonner la sauvegarde et la restauration d'une application VSS, quelles que soient les fonctions de cette dernière. Ce service collabore avec l'application de sauvegarde, les modules d'écriture, les fournisseurs de copie miroir et le noyau du système d'exploitation pour permettre la gestion des copies miroir des volumes et des jeux de copies.
Voir aussi copie miroir, fournisseur de copie miroir, réplique et module d'écriture.

miroir d'objet

Copie d'un objet sauvegarde créé à l'aide de la mise en miroir d'objet. Les miroirs d'objets sont souvent appelés des copies d'objets.

miroir de premier niveau

(terme propre à HP P9000 XP Array Family) Miroir d'un disque interne (LDEV) d'une baie de disques HP StorageWorks P9000 XP Disk Array Family qui peut être lui-même mis en mémoire pour produire des miroirs de second niveau. Pour les tâches de restauration instantanée et de sauvegarde avec temps d'indisponibilité nul Data Protector, vous pouvez seulement utiliser des miroirs de premier niveau.
Voir aussi volume principal et numéro d'unité miroir (MU).

miroir *(terme propre à EMC Symmetrix et à HP P9000 XP Array Family)*

Voir volume cible.

mirrorclone

(terme propre à HP P6000 EVA Array Family) Réplique dynamique d'un volume de stockage, qui est constamment mise à jour en fonction des modifications apportées au volume de stockage d'origine par le biais d'un lien de réplication locale. La réplication entre le volume de stockage d'origine et son mirrorclone peut être suspendue. Pour chaque volume de stockage, il est possible de créer un mirrorclone unique sur la baie de disques.

mise au coffre de supports

Procédé consistant à stocker des supports dans un emplacement sécurisé et distant. Les supports sont retournés au "centre de données" lorsqu'une restauration de données est nécessaire ou lorsqu'ils sont prêts à être réutilisés pour d'autres sauvegardes. La façon dont la mise au coffre est réalisée dépend de la stratégie de sauvegarde adoptée par votre entreprise et de sa politique de protection et de fiabilité de données.

Mise en miroir LVM

Un LVM (Logical Volume Manager), ou gestionnaire de volume logique, est un sous-système permettant de structurer l'espace disque physique et de le mettre en correspondance avec les volumes logiques sur les systèmes UNIX. Un système LVM est constitué de plusieurs groupes de volumes, comportant chacun plusieurs volumes.

MMD

Le processus (service) MMD (Media Management Daemon), démon de gestion des supports, s'exécute sur le Gestionnaire de cellule Data Protector, et contrôle les opérations des périphériques et la gestion des supports. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.

MMDB

La base de données de gestion des supports (MMDB) fait partie de la base de données IDB, laquelle contient les informations concernant les supports, les pools de supports, les périphériques, les bibliothèques, les lecteurs de bibliothèques et les emplacements configurés dans la cellule, ainsi que les supports Data Protector utilisés pour la sauvegarde. Dans un environnement de sauvegarde d'entreprise, cette partie de la base de données peut être commune à toutes les cellules.
Voir aussi CMMDB et CDB.

mode compatible VSS

(terme propre au fournisseur HP P9000 XP Array Family VSS)
L'un des deux modes de fonctionnement du fournisseur matériel P9000 XP Array VSS. Lorsque le fournisseur P9000 XP Array est en mode compatible VSS, le volume source (P-VOL) et sa réplique (S-VOL) sont en mode simplex et dissociés après une sauvegarde. Par conséquent, le nombre de répliques (S-VOL par P-VOL) en rotation n'est pas limité. Pour ce type de configuration, la restauration à partir d'une sauvegarde est possible uniquement par le biais d'un changement de disques.
Voir aussi mode resynchronisation, volume source, volume principal (P-VOL), réplique, volume secondaire (S-VOL) et rotation des jeux de répliques.

mode resynchronisation

(terme propre au fournisseur HP P9000 XP Array Family VSS)
L'un des deux modes de fonctionnement du fournisseur matériel P9000 XP Array VSS. Lorsque le fournisseur P9000 XP Array est en mode resynchronisation, le volume source (P-VOL) et sa réplique (S-VOL) sont en relation de miroir suspendue après une sauvegarde. Le nombre maximum de répliques (S-VOL par P-VOL) faisant l'objet d'une rotation est de trois, à condition que la plage de MU soit de 0-2 ou de 0, 1, 2. La restauration d'une sauvegarde dans ce type de configuration est seulement possible par le biais d'une resynchronisation d'un S-VOL avec son P-VOL.
Voir aussi mode compatible VSS, volume source, volume principal (P-VOL), réplique, volume secondaire (S-VOL), numéro d'unité miroir (MU) et rotation des jeux de répliques.

module d'écriture *(terme propre à Microsoft VSS)* Processus initiant la modification des données sur le volume d'origine. Les modules d'écriture sont généralement des applications ou des services système rédigeant des informations permanentes sur un volume. Ils participent également au processus de synchronisation des copies miroir en assurant la cohérence des données.

module fournisseur d'informations sur les modifications *(terme propre à Windows)* Module pouvant être interrogé pour déterminer quels objets d'un système de fichiers ont été créés, modifiés ou supprimés.

MoM Plusieurs cellules peuvent être regroupées et gérées depuis une cellule centrale. Le système de gestion de la cellule centrale est le Manager-of-Managers (MoM). Les cellules sont appelées clients MoM. Vous pouvez ainsi configurer et gérer plusieurs cellules à partir d'un point central.

moteur de stockage extensible (ESE, pour Extensible Storage Engine) *(terme propre à Microsoft Exchange Server)* Technologie de base de données servant de système de stockage pour les échanges d'informations avec le serveur Microsoft Exchange.

MSM Le Gestionnaire de session de supports (Media Session Manager) de Data Protector s'exécute sur le Gestionnaire de cellule et régit les sessions de supports, telles que la copie de supports.

niveau de journalisation Le niveau de journalisation indique le nombre de détails concernant les fichiers et répertoires qui sont écrits dans la base de données interne (IDB) pendant la sauvegarde, la copie ou la consolidation d'objets. Vous pouvez toujours restaurer vos données, sans tenir compte du niveau de journalisation utilisé pendant la sauvegarde. Data Protector propose quatre niveaux de journalisation : Journaliser tout, Journaliser répertoires, Journaliser fichiers, Pas de journalisation. Les différents paramètres de niveau de journalisation influencent la croissance de l'IDB, la vitesse de sauvegarde et la facilité d'exploration des données à restaurer.

nom de verrouillage Vous pouvez configurer plusieurs fois le même périphérique physique avec des caractéristiques différentes en utilisant des noms de périphérique distincts. Le nom de verrouillage est une chaîne spécifiée par l'utilisateur servant à verrouiller toute

configuration de périphérique de ce type afin d'empêcher un conflit si plusieurs de ces périphériques (noms de périphériques) sont utilisés simultanément. Utilisez un nom de verrouillage identique pour toutes les définitions de périphériques utilisant le même périphérique physique.

numéro d'unité miroir (MU) *(terme propre à HP P9000 XP Array Family)* Nombre entier non négatif qui détermine un volume secondaire (S-VOL) d'un disque interne (LDEV) situé sur une baie de disques HP StorageWorks P9000 XP Disk Array Family.
Voir aussi miroir de premier niveau.

obdrindex.dat *Voir* fichier de récupération de l'IDB.

objet *Voir* objet sauvegarde.

objet d'intégration Un objet sauvegarde d'une intégration Data Protector, telle que Oracle ou SAP DB.

objet sauvegarde Unité de sauvegarde contenant tous les éléments sauvegardés d'un volume de disque (disque logique ou point de montage). Les éléments sauvegardés peuvent être des fichiers, des répertoires ou l'ensemble du disque ou du point de montage. En outre, un objet sauvegarde peut être une entité de base de données/d'application ou une image disque (rawdisk).
Un objet sauvegarde est défini comme suit :

- Nom de client : nom d'hôte du client Data Protector dans lequel l'objet sauvegarde est hébergé.
- Point de montage : pour des objets système de fichiers — point d'accès dans une structure de répertoires (lecteur sous Windows et point de montage sous UNIX) sur le client contenant l'objet sauvegarde. Pour des objets intégration — identificateur du flux de sauvegarde, indiquant les éléments base de données/application sauvegardés.
- Description : Pour les objets système de fichiers — définit exclusivement les objets avec un nom de client et un point de montage identiques. Pour les objets d'intégration — affiche le type d'intégration (SAP ou Lotus, par exemple).
- Type : Type de l'objet sauvegarde. Pour les objets système de fichiers — type de système de fichiers (WinFS, par exemple). Pour les objets intégration — "Bar".

objet, copie

Processus de copie des versions d'objet sélectionnées sur un jeu de supports spécifique. Vous pouvez sélectionner pour la copie des versions d'objet d'une ou de plusieurs sessions de sauvegarde.

objets, mise en miroir

Processus consistant à écrire les mêmes données sur plusieurs jeux de supports au cours d'une session de sauvegarde. Data Protector vous permet de mettre en miroir tous les objets sauvegarde ou certains seulement sur un ou plusieurs jeux de supports.

ON-Bar

(terme propre à Informix Server) Système de sauvegarde et de restauration pour Informix Server. ON-Bar vous permet de créer une copie des données Informix Server et de les restaurer ultérieurement. Le système de sauvegarde et de restauration ON-Bar nécessite l'intervention des composants suivants :

- la commande `onbar`,
- Data Protector en tant que solution de sauvegarde,
- l'interface XBSA,
- les tables de catalogue ON-Bar qui servent à sauvegarder les dbobjects et à effectuer le suivi des instances de dbobjects dans plusieurs sauvegardes.

ONCONFIG

(terme propre à Informix Server) Variable d'environnement spécifiant le nom du fichier de configuration ONCONFIG actif. En cas d'absence de la variable d'environnement ONCONFIG, Informix Server utilise les valeurs de configuration du fichier `onconfig` dans le répertoire `INFORMIXDIR\etc` (sous Windows) ou `INFORMIXDIR/etc/` (sous UNIX).

opérateurs booléens

Les opérateurs booléens pour la fonction de recherche sur le texte entier du système d'aide en ligne sont AND, OR, NOT et NEAR (ET, OU, NON et PROCHE). Utilisés lors d'une recherche, ils vous permettent de définir précisément votre requête en établissant une relation entre les termes de la recherche. Si vous ne spécifiez aucun opérateur dans une recherche comportant plusieurs termes, l'opérateur AND est utilisé par défaut. Par exemple, la requête récupération après sinistre manuelle est identique à récupération AND après AND sinistre AND manuelle.

opération hors contrôle ou sans surveillance Sauvegarde ou restauration ayant lieu en dehors des heures normales de bureau, ce qui signifie qu'aucun opérateur n'est présent pour utiliser l'application de sauvegarde ou les demandes de montage de service, par exemple.

opération sans surveillance *Voir* opération hors contrôle.

Oracle Data Guard *(terme propre à Oracle)* Oracle Data Guard est la principale solution de récupération après sinistre d'Oracle. Oracle Data Guard peut gérer jusqu'à neuf bases de données en attente (auxiliaires), chacune constituant une copie en temps réel de la base de données de production (principale), pour protéger contre les altérations, les corruptions de données, les erreurs humaines et les sinistres. En cas de problème de la base de données de production, le basculement sur l'une des bases de données en attente est possible, celle-ci devenant alors la nouvelle base de données principale. En outre, le temps d'indisponibilité prévu pour la maintenance peut être réduit, car il est possible de faire rapidement basculer le traitement de production de la base de données principale actuelle sur une base de données en attente, et inversement ensuite.

ORACLE_SID *(terme propre à Oracle)* Nom unique pour une instance de serveur Oracle. Pour passer d'un serveur Oracle à un autre, spécifiez le `ORACLE_SID` voulu. Le `ORACLE_SID` est inséré dans les parties CONNECT DATA du descripteur de connexion d'un fichier `TNSNAMES.ORA` et dans la définition du listener TNS du fichier `LISTENER.ORA`.

package *(terme propre à MC/ServiceGuard et Veritas Cluster)* Ensemble de ressources (par exemple, groupes de volumes, services d'applications, noms et adresses IP) nécessaires à l'exécution d'applications compatibles cluster spécifiques.

paquet magique *Voir* Wake ONLAN.

parallélisme Concept consistant à lire plusieurs flux de données depuis une base de données en ligne.

parallélisme de bases de données Plusieurs bases de données sont sauvegardées en même temps si le nombre de périphériques disponibles permet d'effectuer des sauvegardes en parallèle.

parcours de l'arborescence de fichiers

(terme propre à Windows) Processus consistant à parcourir un système de fichiers pour déterminer quels objets ont été créés, modifiés ou supprimés.

partage de charge

Par défaut, Data Protector équilibre automatiquement la charge (l'utilisation) des périphériques sélectionnés pour la sauvegarde, afin que ces derniers soient utilisés de manière uniforme. Ce procédé permet d'optimiser l'utilisation des périphériques en équilibrant le nombre d'objets écrits sur chacun. Cette opération s'effectue automatiquement pendant la sauvegarde ; vous ne devez donc pas gérer la sauvegarde des données il lui suffit de spécifier les périphériques à utiliser. Si vous ne souhaitez pas utiliser le partage de charge, vous pouvez sélectionner le périphérique à utiliser avec chaque objet dans la spécification de sauvegarde. Data Protector accèdera aux périphériques dans l'ordre spécifié.

passage

Voir basculement.

périphérique

Unité physique contenant soit un lecteur, soit une unité plus complexe (une bibliothèque par exemple).

périphérique cible (R2)

(terme propre à EMC Symmetrix) Périphérique EMC Symmetrix prenant part aux opérations SRDF avec un périphérique source (R1). Il réside sur l'unité EMC Symmetrix distante. Il est apparié à un périphérique source (R1) dans l'unité EMC Symmetrix locale et reçoit toutes les données écrites sur le périphérique dont il est le miroir. Pendant les opérations d'E/S courantes, les applications utilisateur ne peuvent accéder à ce périphérique cible. Tout périphérique R2 doit être affecté à un type de groupe RDF2.
Voir aussi périphérique source (R1).

périphérique compatible OBDR

Périphérique pouvant émuler un lecteur de CD-ROM. Chargé à l'aide d'un disque amorçable, il peut être utilisé en tant que périphérique de sauvegarde ou d'amorçage dans le cadre de la récupération après sinistre.

périphérique de bibliothèque de fichiers

Périphérique résidant sur un disque qui fonctionne comme une bibliothèque avec plusieurs supports et contient donc plusieurs fichiers appelés dépôts de fichier.

périphérique de bibliothèque de stockage

Périphérique composé de plusieurs emplacements destinés à stocker des supports optiques ou des fichiers. Lorsqu'il est utilisé pour le stockage de fichiers, le périphérique de bibliothèque de stockage est appelé “périphérique de bibliothèque de stockage de fichiers”.

périphérique de bibliothèque de stockage de fichiers

Périphérique résidant sur un disque et constitué de plusieurs emplacements utilisés pour le stockage de fichiers.

périphérique de fichier autonome

Un périphérique de fichier est un fichier dans un répertoire spécifié vers lequel vous sauvegardez des données.

périphérique de sauvegarde

Périphérique configuré pour une utilisation avec Data Protector, capable d'écrire et de lire des données sur un support de stockage. Il peut sagir, par exemple, d'un lecteur DDS/DAT autonome ou d'une bibliothèque.

périphérique en mode continu

On dit d'un périphérique qu'il fonctionne en mode continu s'il peut fournir un volume de données suffisant au support pour que ce dernier fonctionne en continu. Dans le cas contraire, l'avancement de la bande doit être interrompu, le périphérique attend d'avoir reçu d'autres données, fait légèrement reculer la bande, puis reprend l'écriture des données, et ainsi de suite. En d'autres termes, si le taux auquel les données sont écrites sur la bande est inférieur ou égal à celui auquel elles sont fournies au périphérique par le système informatique, le périphérique fonctionne en mode continu. Ce procédé améliore considérablement les performances du périphérique et la gestion de l'espace de stockage.

périphérique physique

Unité physique contenant soit un lecteur, soit une unité plus complexe (une bibliothèque par exemple).

périphérique source (R1)

(terme propre à EMC Symmetrix) Périphérique EMC Symmetrix prenant part aux opérations SRDF avec un périphérique cible (R2). Toutes les données écrites sur ce périphérique sont mises en miroir sur un périphérique cible (R2) d'une unité EMC Symmetrix distante. Tout périphérique R1 doit être affecté à un type de groupe RDF1.
Voir aussi périphérique cible (R2).

phase 0 de la récupération après sinistre
Préparation à la récupération après sinistre. Il s'agit d'une condition préalable à la réussite de la récupération après sinistre.

phase 1 de la récupération après sinistre
Installation et configuration du DR OS (système d'exploitation de récupération après sinistre) visant à établir la structure de stockage existant précédemment.

phase 2 de la récupération après sinistre
Restauration du système d'exploitation (avec toutes les données de configuration qui définissent l'environnement) et de Data Protector.

phase 3 de la récupération après sinistre
Restauration des données utilisateur et d'application.

Planificateur
Fonction permettant de contrôler le moment et la fréquence des sauvegardes automatiques. En configurant une planification, vous pouvez automatiser le lancement des sauvegardes.

point d'analyse
(terme propre à Windows) Attribut contrôlé par le système et pouvant être associé à tout répertoire ou fichier. La valeur d'un attribut d'analyse peut comporter des données définies par l'utilisateur. Le format des données est reconnu par l'application sur laquelle elles étaient stockées et par un filtre de système de fichiers installé dans le but de permettre l'interprétation des données et le traitement des fichiers. Chaque fois que le système de fichiers rencontre un fichier comportant un point d'analyse, il tente de trouver le filtre de système de fichiers associé au format des données.

point de montage
Point d'accès à un disque ou à un volume logique dans une structure de répertoires, par exemple `/opt` ou `d:`. Sous UNIX, les points de montage sont accessibles au moyen de la commande `bdf` ou `df`.

point de montage de volume
(terme propre à Windows) Répertoire vide sur un volume pouvant être utilisé pour le montage d'un autre volume. Le point de montage de volume sert de passerelle vers le volume cible. Une fois le volume monté, les utilisateurs et les applications peuvent consulter les données stockées sur celui-ci par le chemin d'accès au système de fichiers complet (fusionné), comme si les deux volumes ne faisaient qu'un.

Pont FC *Voir* Pont Fibre Channel.

Pont Fibre Channel Un pont ou multiplexeur Fibre Channel permet de réaliser une migration des périphériques SCSI parallèles existants, tels que les baies de disques RAID, les disques SSD et les bibliothèques de bandes vers un environnement Fibre Channel. Une interface Fibre Channel se trouve à une extrémité du pont ou multiplexeur. Des ports SCSI parallèles se trouvent à l'autre extrémité. La passerelle permet le transfert des paquets SCSI entre les périphériques Fibre Channel et SCSI parallèles.

pool de supports Ensemble de supports du même type (DDS par exemple), utilisé et suivi comme un groupe. Les supports sont formatés et affectés à un pool de supports.

pool libre Source auxiliaire de supports utilisée par les pools n'ayant plus aucun support disponible. Les pools de supports doivent être configurés pour l'utilisation de pools libres.

pool smart copy *(terme propre à VLS)* Pool définissant quels emplacement de la bibliothèque de destination sont disponibles au titre de cibles Smart Copy pour une bibliothèque virtuelle source spécifiée. *Voir aussi* Système de bibliothèque virtuelle (VLS) et copie intelligente.

post-exécution Option de sauvegarde qui exécute une commande ou un script après la sauvegarde d'un objet ou une fois que la session de sauvegarde est terminée. Les commandes de post-exécution ne sont pas fournies avec Data Protector. L'utilisateur doit les créer lui-même. Elles peuvent être rédigées sous la forme de programmes exécutables ou de fichiers séquentiels sous Windows, ou bien de scripts shell sous UNIX.
Voir aussi pré-exécution.

pré-exécution Option de sauvegarde qui exécute une commande ou un script avant la sauvegarde d'un objet ou avant que la session de sauvegarde ne démarre. Les commandes de pré-exécution ne sont pas fournies avec Data Protector. L'utilisateur doit les créer lui-même. Elles peuvent être rédigées sous la forme de programmes exécutables ou de fichiers séquentiels sous Windows, ou bien de scripts shell sous UNIX.
Voir aussi post-exécution.

processus BC

(terme propre à EMC Symmetrix) Solution d'environnement de stockage protégé dans le cadre de laquelle des périphériques EMC Symmetrix ont été spécialement configurés en tant que miroirs ou volumes CB pour protéger les données stockées sur des périphériques EMC Symmetrix standard.
Voir aussi BCV.

Profil utilisateur

(terme propre à Windows) Informations de configuration définies pour chaque utilisateur. Ces informations comprennent la configuration du bureau, les couleurs d'écran, les connexions réseau, etc. Lorsqu'un utilisateur se connecte, le système charge son profil et l'environnement Windows le prend en compte.

propriétaire de la sauvegarde

Tout objet sauvegarde de la base de données IDB a un propriétaire. Par défaut, le propriétaire d'une sauvegarde est l'utilisateur qui lance la session de sauvegarde.

propriété

La propriété de sauvegarde agit sur la capacité des utilisateurs à voir et à restaurer les données. Chaque session de sauvegarde, avec toutes les données sauvegardées qu'elle contient, est affectée à un propriétaire. Il peut s'agir de l'utilisateur qui lance une sauvegarde interactive, du compte sous lequel le processus CRS est exécuté ou de l'utilisateur désigné comme propriétaire dans les options de la spécification de sauvegarde.
Si un utilisateur démarre une spécification de sauvegarde existante sans la modifier, la session n'est pas considérée comme interactive.
Si une spécification de sauvegarde modifiée est démarrée par un utilisateur, celui-ci est le propriétaire, à moins que les conditions ci-après soient remplies :

- L'utilisateur possède le droit utilisateur Permuter propriété de session.
- Le propriétaire d'une session de sauvegarde est explicitement défini dans la spécification de sauvegarde, avec le nom d'utilisateur, le groupe, le nom de domaine et le nom du système.

Si vous prévoyez d'effectuer une sauvegarde sur un Gestionnaire de cellule UNIX, le propriétaire de la session est root:sys à moins que les conditions indiquées ci-dessus ne soient remplies.
Si vous prévoyez d'effectuer une sauvegarde sur un Gestionnaire de cellule Windows, le propriétaire de la session est l'utilisateur

spécifié lors de l'installation, à moins que les conditions indiquées ci-dessus soient remplies.
Lors de la copie ou de la consolidation d'objets, le propriétaire est par défaut l'utilisateur qui démarre l'opération, sauf si un autre propriétaire est défini dans la spécification de copie ou de consolidation.

protection

Voir protection des données et également protection de catalogue.

protection de catalogue

Permet de définir le temps de conservation des informations concernant les données sauvegardées (noms et versions de fichiers) dans la base de données IDB.
Voir aussi protection des données.

pulsation

Ensemble de données de cluster qui comporte un horodatage contenant des informations sur l'état de fonctionnement d'un nœud de cluster spécifique. Cet ensemble de données est distribué à tous les nœuds de cluster.

quota de disque

Concept permettant de gérer l'utilisation de l'espace disque pour l'ensemble des utilisateurs ou pour certains d'entre eux sur un système informatique. Plusieurs plates-formes de système d'exploitation utilisent ce concept.

quotas de disque utilisateur

Le support de gestion des quotas NTFS permet le contrôle et le suivi élaboré de l'utilisation de l'espace disque sur les volumes de stockage partagés. Data Protector sauvegarde des quotas de disque utilisateur sur l'ensemble du système et pour tous les utilisateurs configurés à un instant donné.

RAID

Ensemble redondant de disques indépendants (Redundant Array of Independent Disks).

rapport d'audit

Sortie lisible par l'utilisateur d'informations d'audit créées à partir des données stockées dans les fichiers journaux d'audit.

RCU

Voir Unité de télécommande (RCU).

RDF1/RDF2

(terme propre à EMC Symmetrix) Type de groupe de périphériques SRDF. Seuls les périphériques RDF peuvent être attribués à un groupe RDF. Le type de groupe RDF1 contient des périphériques sources (R1) et le type de groupe RDF2 des périphériques cibles (R2).

RDS Le processus RDS (Raima Database Server) s'exécute sur le Gestionnaire de cellule Data Protector et gère la base de données IDB. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.

RecoveryInfo Lors de la sauvegarde de fichiers de configuration Windows, Data Protector collecte les informations sur la configuration système actuelle (volume, configuration disque et réseau). Ces informations sont nécessaires pour la récupération après sinistre.

récupération après sinistre Procédé permettant de restaurer le disque du système principal d'un client dans un état proche de celui dans lequel il se trouvait après une sauvegarde complète.

récupération en ligne La récupération en ligne s'exécute lorsque le Gestionnaire de cellule est accessible. Dans ce cas, la plupart des fonctionnalités de Data Protector sont disponibles (le Gestionnaire de cellule exécute la session, les sessions de restauration sont consignées dans l'IDB, vous pouvez suivre l'avancement de la restauration via l'interface utilisateur, etc.).

récupération hors ligne Ce type de récupération est exécuté si le Gestionnaire de cellule est inaccessible, en raison de problèmes réseau, par exemple. Seuls les périphériques autonomes et les périphériques de bibliothèque SCSI peuvent être utilisés pour une récupération hors ligne. La récupération du Gestionnaire de cellule s'effectue toujours hors ligne.

récupération locale et distante La récupération distante s'effectue lorsque tous les hôtes de l'Agent de support spécifiés dans le fichier SRD sont accessibles. Si l'un d'entre eux échoue, le processus de récupération après sinistre bascule du mode distant au mode local. Dans ce cas, une recherche est exécutée sur les périphériques connectés en local au système cible. Si la recherche ne renvoie qu'un seul périphérique, celui-ci sera automatiquement utilisé. Dans le cas contraire, Data Protector vous invitera à sélectionner le périphérique à utiliser pour la restauration.

récupération matérielle *(terme propre à Microsoft Exchange Server)* Récupération de la base de données Microsoft Exchange Server effectuée après une restauration par le moteur de base de données, au moyen des fichiers journaux de transactions.

recyclage ou suppression de la protection
Processus consistant à supprimer la protection de toutes les données sauvegardées se trouvant sur le support, autorisant ainsi Data Protector à les écraser au cours de l'une des sauvegardes ultérieures. Les données provenant de la même session, mais se trouvant sur d'autres supports, ne sont plus protégées non plus. Le recyclage ne modifie pas les données enregistrées sur le support.

réécriture
Option définissant un mode de résolution de conflits pendant la restauration. Tous les fichiers sauvegardés sont restaurés, même s'ils sont plus anciens que les fichiers existants.
Voir aussi fusion.

Registre Windows
Base de données centralisée utilisée par Windows pour stocker les informations de configuration du système d'exploitation et des applications installées.

répertoire DC
Le répertoire de catalogue des détails (DC) contient des fichiers binaires DC où sont stockées les informations relatives aux versions de fichier. Il constitue la partie DCBF de la base de données IDB, dont il occupe environ 80 %. Le répertoire DC par défaut est intitulé `dcbf` et se trouve sur le Gestionnaire de cellule, dans le répertoire données_programme_Data_Protector\db40 (Windows Server 2008), `répertoire_Data_Protector\db40` (autres systèmes Windows) ou `/var/opt/omni/server/db40` (systèmes UNIX). Vous pouvez cependant en créer davantage et utiliser un emplacement de votre choix. Chaque cellule peut gérer jusqu'à 50 répertoires DC. Par défaut, la taille maximale d'un répertoire DC est de 16 Go.

répertoire_Data_Protector
Sous Windows Vista, Windows 7 et Windows Server 2008, il s'agit du répertoire contenant les fichiers de programme Data Protector. Sur les autres systèmes Windows, c'est le répertoire contenant les fichiers de données et de programme Data Protector. Le chemin par défaut est `%ProgramFiles%\OmniBack`, mais vous pouvez le modifier dans l'assistant d'installation de Data Protector au moment de l'installation.
Voir aussi données_programme_Data_Protector.

réplique
(terme propre à ZDB) Une image, à un instant T, des données des volumes sources qui contiennent les objets sauvegarde spécifiques à l'utilisateur. En fonction du matériel/logiciel avec lequel elle est créée, l'image peut être un doublon exact

indépendant (clone) des blocs de stockage au niveau du disque physique (split mirror, par exemple) ou bien une copie virtuelle (par exemple, un snapshot). Du point de vue d'un système d'exploitation de base, le disque physique contenant les objets sauvegarde est répliqué dans son intégralité. Toutefois, si un gestionnaire de volume est utilisé sur UNIX, le groupe entier de volumes ou de disques contenant un objet sauvegarde (volume logique) est dupliqué. Si des partitions sont utilisées sous Windows, c'est l'ensemble du volume physique contenant la partition sélectionnée qui est répliqué.
Voir aussi snapshot, création de snapshot, split mirror et création de split mirror.

restauration incrémentale

(terme propre à EMC Symmetrix) Opération de contrôle BCV ou SRDF. Dans les opérations de contrôle BCV, une restauration incrémentale réaffecte un périphérique BCV comme miroir disponible suivant du périphérique standard de la paire. Cependant, les périphériques standard sont mis à jour uniquement avec les données écrites sur le périphérique BCV au cours de la séparation des paires d'origine ; les données écrites sur le périphérique standard au cours de la séparation sont écrasées par les données du miroir BCV. Dans les opérations de contrôle SRDF, une restauration incrémentale réaffecte un périphérique (R2) cible comme miroir disponible suivant du périphérique (R1) source de la paire. Cependant, les périphériques (R1) sources sont mis à jour uniquement avec les données écrites sur le périphérique (R2) cible au cours de la séparation des paires d'origine ; les données écrites sur le périphérique (R1) source au cours de la séparation sont écrasées par les données du miroir (R2) cible.

restauration instantanée

(terme propre à la sauvegarde ZDB) Processus qui utilise une réplique, générée par une session ZDB sur disque ou ZDB sur disque + bande, pour restaurer le contenu des volumes sources dans l'état dans lequel ils étaient au moment de la création de la réplique. Cela évite d'avoir à exécuter une restauration à partir d'une bande. Selon l'application ou la base de données concernée, ce processus est suffisant, ou d'autres étapes peuvent être nécessaires pour une récupération complète, par exemple l'application de fichiers journaux de transactions.
Voir aussi réplique, sauvegarde avec temps d'indisponibilité nul (ZDB), sauvegarde ZDB sur disque et sauvegarde ZDB sur disque + bande.

restauration parallèle

Procédé consistant à restaurer simultanément (c'est-à-dire en parallèle) des données sauvegardées vers plusieurs disques, en exécutant pour cela plusieurs Agents de disque qui reçoivent des données d'un Agent de support. Pour que la restauration parallèle fonctionne, les données sélectionnées doivent se trouver sur des disques ou volumes logiques différents, et lors de la sauvegarde, les données provenant des différents objets doivent avoir été envoyées au même périphérique avec deux Agents de disque ou plus. Pendant une restauration parallèle, les données concernant les différents objets à restaurer sont lues simultanément sur les supports, améliorant ainsi les performances du système.

restauration Split Mirror

(terme propre à EMC Symmetrix et à HP P9000 XP Array Family) Processus dans lequel les données sauvegardées lors d'une session de sauvegarde ZDB sur bande ou ZDB sur disque + bande sont d'abord copiées à partir des supports de sauvegarde vers une réplique, puis à partir de la réplique vers les volumes sources. Les objets sauvegarde individuels ou les sessions complètes peuvent être restauré(e)s à l'aide de cette méthode.
Voir aussi sauvegarde ZDB sur bande, ZDB sur disque + bande et réplique.

RMAN *(terme propre à Oracle)*

Voir Gestionnaire de récupération.

rotation des jeux de répliques

(terme propre à ZDB) Utilisation d'un jeu de répliques pour la génération régulière de sauvegardes : chaque fois qu'une même spécification de sauvegarde nécessitant l'utilisation d'un jeu de répliques est exécutée, une nouvelle réplique est créée puis ajoutée au jeu, tant que le nombre maximum de répliques fixé pour le jeu n'est pas atteint. Une fois ce nombre atteint, la réplique la plus ancienne du jeu est écrasée.
Voir aussi réplique et jeu de répliques.

rotation des miroirs *(terme propre à HP P9000 XP Array Family)*

Voir rotation des jeux de répliques.

RSM

Le Gestionnaire de session de restauration (Restore Session Manager) Data Protector contrôle les sessions de restauration

et de vérification d'objet. Ce processus est toujours exécuté sur le système du Gestionnaire de cellule.

RSM

(terme propre à Windows) Le RSM (Removable Storage Manager), ou Gestionnaire de supports amovibles, comprend un service de gestion des supports facilitant la communication entre les applications, les changeurs robotiques et les bibliothèques de supports. Il permet à plusieurs applications de partager des bibliothèques de supports robotiques locales et des lecteurs de disques ou de bandes, et de gérer les supports amovibles.

SAPDBA

(terme propre à SAP R/3) Interface utilisateur SAP R/3 intégrant les outils BRBACKUP, BRARCHIVE et BRRESTORE.

sauvegarde avec temps d'indisponibilité nul (ZDB)

Approche de sauvegarde selon laquelle les techniques de duplication des données fournies par une baie de disques permettent de réduire l'impact des opérations de sauvegarde sur un système d'application. Une réplique des données à sauvegarder est tout d'abord créée. Toutes les opérations de sauvegarde suivantes sont effectuées au niveau des données répliquées plutôt que les données d'origine, le système d'application pouvant retourner en mode de fonctionnement normal.
Voir aussi sauvegarde ZDB sur disque, sauvegarde ZDB sur bande, ZDB sur disque + bande et restauration instantanée.

sauvegarde complète

Sauvegarde au cours de laquelle tous les objets sélectionnés sont sauvegardés, qu'ils aient été ou non modifiés récemment.
Voir aussi types de sauvegarde.

sauvegarde complète synthétique

Résultat d'une opération de consolidation d'objet, au cours de laquelle une chaîne de restauration d'un objet sauvegarde est fusionnée en une nouvelle version complète synthétique de cet objet. En termes de vitesse de restauration, une telle sauvegarde est équivalente à une sauvegarde complète classique.

sauvegarde complète virtuelle

Type de sauvegarde synthétique efficace au cours de laquelle les données sont consolidées à l'aide de pointeurs au lieu d'être copiées. Elle est réalisée si toutes les sauvegardes (la sauvegarde complète, les sauvegardes incrémentales et la sauvegarde complète virtuelle résultante) sont écrites dans une seule bibliothèque de fichiers qui utilise le format de support de fichiers distribués.

sauvegarde d'image disque (rawdisk)

Sauvegarde ultra-rapide au cours de laquelle Data Protector sauvegarde les fichiers en tant qu'images bitmap. Ce type de sauvegarde (rawdisk) ne suit pas la structure des fichiers et des répertoires stockés sur le disque ; elle stocke la structure de l'image disque au niveau des octets. Vous pouvez effectuer une sauvegarde d'image disque de certaines sections du disque ou de sa totalité.

sauvegarde de base de données complète

Sauvegarde de toutes les données d'une base de données, et non uniquement des données ayant été modifiées après la dernière sauvegarde (complète ou incrémentale) de la base de données. Une sauvegarde complète de base de données ne dépend d'aucune autre sauvegarde.

sauvegarde de base de données différentielle

Sauvegarde de base de données au cours de laquelle ne sont sauvegardées que les modifications intervenues après la dernière sauvegarde complète de la base.

sauvegarde de boîte au lettres complète

La sauvegarde complète de boîte aux lettres consiste à sauvegarder tout le contenu d'une boîte aux lettres.

sauvegarde de client

Sauvegarde de tous les volumes (systèmes de fichiers) montés sur un client Data Protector. Ce qui est sauvegardé est fonction du mode de sélection des objets dans une spécification de sauvegarde :

- Si vous cochez la case située en regard du nom du système client, un objet sauvegarde unique de type `système client` est créé. Par conséquent, lors de la sauvegarde, Data Protector détecte d'abord tous les volumes montés sur le client sélectionné, puis les sauvegarde. Sur les clients Windows, la `CONFIGURATION` est également sauvegardée.
- Si vous sélectionnez individuellement tous les volumes montés sur le système client, un objet sauvegarde séparé de type `Système de fichiers` est créé pour chaque volume. Ainsi, au moment de la sauvegarde, seuls les volumes sélectionnés sont sauvegardés. Les volumes qui ont été potentiellement montés sur le client après la création de la spécification de sauvegarde ne sont pas sauvegardés.

sauvegarde de configuration Windows

Data Protector permet de sauvegarder la CONFIGURATION Windows, y compris le registre Windows, les profils utilisateur,

les journaux d'événements et les données des serveurs WINS et DHCP (sils sont configurés) en une seule étape.

sauvegarde de disque en plusieurs étapes

Le processus de sauvegarde des données en plusieurs étapes permet d'améliorer les performances des sauvegardes et des restaurations, de réduire les coûts de stockage des données sauvegardées et d'améliorer la disponibilité et l'accessibilité des données pour restauration. La procédure consiste à sauvegarder les données sur un type de support (par exemple, un disque), puis à les copier vers un autre type de support (par exemple, une bande).

sauvegarde de snapshot

Voir sauvegarde sur bande ZDB, sauvegarde sur disque ZDB et sauvegarde sur disque+bande ZDB.

sauvegarde de transaction

Les sauvegardes de transaction consomment généralement moins de ressources que les sauvegardes de base de données ; elles peuvent donc être effectuées plus souvent que les sauvegardes de base de données. En effectuant des sauvegardes de transaction, l'utilisateur peut récupérer la base de données telle qu'elle était à un moment précis précédant la survenue d'un problème.

sauvegarde de transaction

(terme propre à Sybase et SQL) Sauvegarde du journal de transactions contenant un enregistrement des modifications effectuées depuis la dernière sauvegarde complète ou la dernière sauvegarde de transaction.

sauvegarde delta

Sauvegarde contenant toutes les modifications apportées à la base de données depuis la dernière sauvegarde, quel qu'en soit le type.
Voir aussi types de sauvegarde.

sauvegarde différentielle

Sauvegarde incrémentale qui permet de sauvegarder les modifications effectuées depuis la dernière sauvegarde complète. Pour procéder à une telle sauvegarde, indiquez le type de sauvegarde Incr1.
Voir aussi sauvegarde incrémentale.

sauvegarde différentielle

(terme propre à Microsoft SQL Server) Sauvegarde de base de données au cours de laquelle seules les modifications intervenues après la dernière sauvegarde complète de la base sont sauvegardées.
Voir aussi types de sauvegarde.

sauvegarde du journal des transactions

Les sauvegardes du journal des transactions consomment généralement moins de ressources que les sauvegardes de base de données ; elles peuvent donc être effectuées plus souvent que les sauvegardes de base de données. En effectuant des sauvegardes des journaux de transactions, l'utilisateur peut récupérer la base de données telle qu'elle était à un moment précis.

sauvegarde en ligne

Une sauvegarde effectuée alors que la base de données est accessible. La base de données passe dans un mode de sauvegarde particulier pendant toute la durée du processus de réplication des données. Pour les sauvegardes sur bande, par exemple, elle est nécessaire jusqu'à ce que le transfert de données vers la bande soit terminé. Pendant ce laps de temps, la base de données continue à être pleinement opérationnelle mais des problèmes de performance mineurs peuvent survenir et la taille des fichiers journaux peut croître très rapidement. Elle reprend son fonctionnement normal avant que les opérations post-sauvegarde potentielles ne démarrent.
Dans certains cas, les journaux de transactions doivent également être sauvegardés pour permettre la restauration d'une base de données cohérente.
Voir aussi sauvegarde avec temps d'indisponibilité nul (ZDB) et sauvegarde hors ligne.

sauvegarde hors ligne

Sauvegarde au cours de laquelle une base de données d'application ne peut pas être utilisée par l'application. Lors d'une session de sauvegarde hors ligne, la base de données est généralement mise en veille, afin de permettre une utilisation par le système de sauvegarde et non par l'application, pendant toute la durée du processus de réplication des données. Pour les sauvegardes sur bande, par exemple, cette mise en veille est effective jusqu'à ce que le transfert de données vers la bande soit terminé. Elle reprend son fonctionnement normal avant que les opérations post-sauvegarde potentielles ne démarrent.
Voir aussi sauvegarde avec temps d'indisponibilité nul (ZDB) et sauvegarde en ligne.

sauvegarde incrémentale

Procédé consistant à ne sauvegarder que les fichiers auxquels des modifications ont été apportées depuis la dernière sauvegarde. Plusieurs niveaux de sauvegarde incrémentale sont disponibles, ce qui permet de contrôler en détail la longueur de la chaîne de restauration.
Voir aussi types de sauvegarde.

sauvegarde incrémentale

(terme propre à Microsoft Exchange Server) Sauvegarde de données Microsoft Exchange Server modifiées depuis la dernière sauvegarde complète ou incrémentale. Avec la sauvegarde incrémentale, seuls les fichiers journaux de transactions sont sauvegardés.
Voir aussi types de sauvegarde.

sauvegarde incrémentale avancée

Une sauvegarde incrémentale classique inclut les fichiers modifiés depuis une sauvegarde précédente, mais présente certaines limites en matière de détection des modifications. Une sauvegarde incrémentale avancée détecte et sauvegarde de manière fiable les fichiers renommés et déplacés, ainsi que ceux dont les attributs ont été modifiés.

sauvegarde incrémentale de boîte aux lettres

Une sauvegarde incrémentale de boîte aux lettres consiste à sauvegarder toutes les modifications apportées à la boîte aux lettres depuis la dernière sauvegarde, quel qu'en soit le type.

sauvegarde incrémentale de boîte aux lettres "incrémentale1"

Une sauvegarde incrémentale1 de boîte aux lettres consiste à sauvegarder toutes les modifications apportées à la boîte aux lettres depuis la dernière sauvegarde complète.

sauvegarde rawdisk

Voir sauvegarde d'image disque.

sauvegarde sans bande *(terme propre à ZDB)*

Voir ZDB sur disque.

sauvegarde Split Mirror *(terme propre à EMC Symmetrix)*

Voir ZDB sur bande.

sauvegarde Split Mirror *(terme propre à HP P9000 XP Array Family)*

Voir sauvegarde sur bande ZDB, sauvegarde sur disque ZDB et sauvegarde sur disque+bande ZDB.

sauvegarde synthétique

Solution de sauvegarde qui produit une sauvegarde complète synthétique, équivalant à une sauvegarde complète classique en termes de données, sans créer de charge sur les serveurs de

production ou le réseau. Une sauvegarde complète synthétique est créée à partir d'une sauvegarde complète précédente et d'un certain nombre de sauvegardes incrémentales.

sauvegarde système sur bande *(terme propre à Oracle)* Interface Oracle chargée d'exécuter les actions nécessaires au chargement, à l'étiquetage et au déchargement des bons périphériques de sauvegarde lorsqu'Oracle émet des demandes de sauvegarde ou de restauration.

sauvegarde ZDB complète Session de sauvegarde ZDB sur bande ou ZDB sur disque + bande au cours de laquelle tous les objets sélectionnés sont copiés sur la bande, même si aucune modification n'a eu lieu depuis la dernière sauvegarde.
Voir aussi sauvegarde ZDB incrémentale.

sauvegarde ZDB incrémentale Session de sauvegarde ZDB sur bande ou ZDB sur disque + bande du système de fichiers au cours de laquelle seules les modifications effectuées depuis la dernière sauvegarde protégée (complète ou incrémentale) sont transférées sur bande.
Voir aussi sauvegarde ZDB complète.

sauvegarde ZDB sur bande *(terme propre à la sauvegarde ZDB)* Type de sauvegarde avec temps d'indisponibilité nul caractérisé par le fait que la réplique créée est copiée en continu sur un support de sauvegarde, généralement une bande. La restauration instantanée étant impossible avec ce type de sauvegarde, la réplique ne doit pas être conservée sur la baie de disques après la sauvegarde. Les données sauvegardées peuvent être restaurées à l'aide de la restauration Data Protector standard à partir d'une bande. Avec certaines familles de baies de disques, la restauration Split Mirror peut aussi être utilisée.
Voir aussi sauvegarde avec temps d'indisponibilité nul (ZDB), sauvegarde ZDB sur disque, sauvegarde ZDB sur disque + bande, restauration instantanée et réplique.

sauvegarde ZDB sur disque *(terme propre à la sauvegarde ZDB)* Type de sauvegarde avec temps d'indisponibilité nul caractérisé par le fait que la réplique créée est conservée sur la baie de disques en tant que sauvegarde des volumes sources à un instant donné. Il est possible de conserver plusieurs répliques, générées avec la même spécification de sauvegarde à des instants différents, dans un jeu de répliques. Le processus de restauration

instantanée permet de restaurer une réplique à partir d'une session ZDB sur disque.
Voir aussi sauvegarde avec temps d'indisponibilité nul (ZDB), sauvegarde ZDB sur bande, ZDB sur disque + bande, restauration instantanée et rotation des jeux de répliques.

sauvegarde ZDB sur disque + bande

(terme propre à la sauvegarde ZDB) Type de sauvegarde avec temps d'indisponibilité nul caractérisé par le fait que la réplique créée est conservée sur la baie de disques en tant que sauvegarde des volumes sources à un instant donné, de la même manière que la sauvegarde ZDB sur disque. Toutefois, les données de la réplique sont également transférées sur un support de sauvegarde, comme lors du processus ZDB sur bande. Si cette méthode de sauvegarde est utilisée, les données sauvegardées dans la même session peuvent être restaurées via le processus de restauration instantanée, la restauration Data Protector standard à partir d'une bande ou, avec certaines familles de baies de disques, la restauration Split Mirror.
Voir aussi sauvegarde avec temps d'indisponibilité nul (ZDB), sauvegarde ZDB sur disque, sauvegarde ZDB sur bande, restauration instantanée, réplique et rotation des jeux de répliques.

script CMD pour Informix Server

(terme propre à Informix Server) Script CMD Windows créé dans INFORMIXDIR lorsqu'une base de données Informix Server est configurée. Le script CMD est un ensemble de commandes système chargé d'exporter les variables d'environnement pour Informix Server.

script shell log_full

(terme propre à Informix Server UNIX) Script fourni par ON-Bar que vous pouvez utiliser pour lancer la sauvegarde des fichiers journaux logiques lorsque Informix Server émet une alarme de saturation de journal. Le paramètre de configuration `ALARMPROGRAM` Informix Server sélectionné par défaut est `REP_INFORMIX/etc/log_full.sh`, où `REP_INFORMIX` est le répertoire de base d'Informix Server. Si vous ne souhaitez pas que les journaux logiques soient sauvegardés en continu, attribuez la valeur `REP_INFORMIX/etc/no_log.sh` au paramètre de configuration `ALARMPROGRAM`.

section PME/PMI

Voir sauvegarde Split Mirror.

serveur d'interface Java

Le serveur de l'interface Java est un composant de l'interface utilisateur graphique Java qui est installé sur le système

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

serveur de base de données Ordinateur sur lequel est stockée une base de données volumineuse, telle qu'une base de données SAP R/3 ou Microsoft SQL. Une base de données stockée sur un serveur est accessible aux clients.

serveur DHCP Système sur lequel s'exécute le protocole DHCP (Dynamic Host Configuration Protocol), permettant l'affectation dynamique des adresses IP et la configuration réseau pour les clients DHCP.

Serveur d'installation Système informatique contenant un référentiel des packages logiciels Data Protector pour une architecture spécifique. Le Serveur d'installation permet l'installation à distance des clients Data Protector. Dans les environnements mixtes, deux serveurs d'installation au moins sont nécessaires : l'un pour les systèmes UNIX et l'autre pour les systèmes Windows.

Serveur DNS Dans le modèle client-serveur DNS, il s'agit du serveur contenant les informations relatives à une partie de la base de données DNS et rendant les noms des ordinateurs accessibles aux programmes de résolution client en faisant une demande de résolution de noms via Internet.

serveur Sybase SQL *(terme propre à Sybase)* Le serveur d'une architecture "client-serveur" Sybase. Le serveur Sybase SQL gère plusieurs bases de données et utilisateurs, assure le suivi des positions physiques des données sur les disques, établit le mappage entre la description logique des données et leur stockage physique et maintient les caches de données et de procédures en mémoire.

serveur virtuel Machine virtuelle dans un environnement de clusters définie sur un domaine par un nom et une adresse IP réseau. Son adresse est mise en cache par le service de cluster et mappée au nœud cluster qui exécute les ressources du serveur virtuel. De cette façon, toutes les demandes concernant un serveur virtuel donné sont mises en cache par un nœud de cluster spécifique.

serveur WINS

Système sur lequel s'exécute le logiciel Windows Internet Name Service chargé de la résolution des noms des ordinateurs du réseau Windows en adresses IP. Data Protector peut sauvegarder les données du serveur WINS dans le cadre de la configuration Windows.

Service de réplication de fichiers (FRS)

Service Windows dupliquant les stratégies de groupe et les scripts d'ouverture de session de la banque du contrôleur de domaine. Ce service duplique également les partages de système de fichiers distribués (DFS) entre des systèmes et permet à tout serveur d'effectuer une opération de réplication.

service de réplication de sites

(terme propre à Microsoft Exchange Server) Service Microsoft Exchange Server 2003 qui offre une compatibilité avec Microsoft Exchange Server 5.5 par l'émulation du service d'annuaire Exchange Server 5.5.
Voir aussi banque d'informations et service Gestionnaire de clés.

service de réplication Exchange

(terme propre à Microsoft Exchange Server) Service Microsoft Exchange Server qui représente les groupes de stockage répliqués au moyen de la technologie LCR (Local Continuous Replication) ou CCR (Cluster Continuous Replication).
Voir aussi Cluster Continuous Replication et Local Continuous Replication.

services Terminal Server

(terme propre à Windows) Les services Terminal Server de Windows fournissent un environnement multi-sessions permettant aux clients d'accéder à des sessions Windows virtuelles ainsi qu'à des applications Windows exécutées sur le serveur.

session

Voir session de sauvegarde, session de gestion de supports et session de restauration.

session de consolidation d'objet

Processus consistant à fusionner une chaîne de restauration d'un objet sauvegarde, constituée d'une sauvegarde complète et d'au moins une sauvegarde incrémentale, en une nouvelle version consolidée de cet objet.

session de copie d'objet

Processus créant une copie supplémentaire des données sauvegardées sur un jeu de supports différent. Au cours de la session, les objets sauvegardés sélectionnés sont copiés du support source vers le support cible.

session de gestion de supports Session servant à exécuter une action sur un support, telle que l'initialisation, l'analyse du contenu, la vérification des données stockées sur le support, ou la copie de ce dernier.

session de restauration Processus permettant de copier les données de supports de sauvegarde vers un client.

session de sauvegarde Processus consistant à créer une copie des données sur un support de stockage. Les activités sont définies dans une spécification de sauvegarde ou dans une session interactive. Tous les clients configurés dans une spécification de sauvegarde sont sauvegardés ensemble lors d'une session de sauvegarde unique, avec le même type de sauvegarde. Une session de sauvegarde génère un jeu de supports sur lesquels des données ont été écrites, également appelé "jeu de sauvegarde" ou "jeu de supports".
Voir aussi spécification de sauvegarde, sauvegarde complète et sauvegarde incrémentale.

session de vérification d'objet Processus qui vérifie l'intégrité des données d'objets sauvegarde ou de versions d'objets spécifiés ainsi que la capacité de sélectionner ou non des composants de réseau Data Protector pour les fournir à un hôte spécifié. Les sessions de vérification d'objet peuvent être exécutées de façon interactive ou conformément à des spécifications automatiques, planifiées ou de post-sauvegarde.

SGBDR Système de gestion de base de données relationnelle.

SIBF Les fichiers SIBF (Serverless Integrations Binary Files), ou fichiers binaires d'intégrations sans serveur, représentent la partie de la base de données IDB stockant les métadonnées brutes NDMP. Ces données sont nécessaires à la restauration des objets NDMP.

simultanéité *Voir* Agents de disque simultanés

SMBF Les fichiers binaires de messages de session (SMBF), un élément de l'IDB (base de données interne), contiennent les messages générés lors des sessions de sauvegarde, de restauration, de copie d'objet, de consolidation d'objet, de vérification d'objet et de gestion des supports. Chaque session génère un fichier binaire. Les fichiers sont regroupés par année et par mois.

snapshot

(terme propre à HP P6000 EVA Array Family, à HP P9000 XP Array Family et à HP StorageWorks P4000 SAN Solutions) Type de volume cible créé à laide dune technologie de réplication spécifique. Selon le modèle de baie de disques et la technique de réplication choisie, plusieurs types de snapshots dotés de caractéristiques différentes sont disponibles. Chaque snapshot peut être soit une copie virtuelle, qui dépend encore du contenu du volume source, soit une copie indépendante (clone) du volume source.
Voir aussi réplique et création de snapshot.

snapshot transportable

(terme propre à Microsoft VSS) Copie miroir créée sur le système d'application et pouvant être présentée au système de sauvegarde où est effectuée une sauvegarde.
Voir aussi Microsoft Volume Shadow Copy Service (VSS).

spécification de sauvegarde

Liste d'objets à sauvegarder avec un ensemble de périphériques ou de lecteurs à utiliser, des options de sauvegarde pour tous les objets de la spécification, et la date et l'heure d'exécution des sauvegardes. Les objets peuvent être des disques/volumes entiers ou une partie de ceux-ci ; il peut s'agir par exemple de fichiers, de répertoires, voire même du registre Windows. L'utilisateur peut définir des listes de sélection de fichiers, telles que les listes d'inclusion ou d'exclusion.

Split Mirror

(terme propre aux baies de disques EMC Symmetrix et à HP P9000 XP Array Family) Type de volume cible créé à l'aide d'une technologie de réplication spécifique. Une réplique Split Mirror fournit des copies indépendantes (clones) des volumes sources.
Voir aussi réplique et création de split mirror.

SRDF

(terme propre à EMC Symmetrix) L'utilitaire SRDF (Symmetrix Remote Data Facility), ou utilitaire de gestion des données distantes Symmetrix, est un processus de continuité des activités permettant de dupliquer efficacement et en temps réel les données des SLD entre plusieurs environnements de traitement séparés. Ces environnements peuvent se trouver au sein d'un même ordinateur ou être séparés par de grandes distances.

stratégie d'allocation de supports

Procédé permettant de déterminer l'ordre d'utilisation des supports pour la sauvegarde. Dans le cas d'une stratégie d'allocation stricte, Data Protector demande un support spécifique. Dans le cas d'une stratégie souple, Data Protector

demande tout support approprié. Dans le cas d'une stratégie de priorité aux supports formatés, Data Protector préfère utiliser les supports inconnus, même si des supports non protégés sont disponibles dans la bibliothèque.

stratégie d'utilisation des supports

La stratégie d'utilisation des supports permet de contrôler la manière dont les nouvelles sauvegardes sont ajoutées aux supports déjà utilisés. Les options sont les suivantes : `Ajout possible`, `Sans possibilité d'ajout` et `Ajout possible aux incrémentales uniquement`.

SYMA *(terme propre à EMC Symmetrix)*

Voir Agent EMC Symmetrix.

système cible

(terme propre à la récupération après sinistre) Système ayant subi un incident informatique. Le système cible est généralement non amorçable et l'objet de la récupération après sinistre consiste justement à redonner à ce système sa configuration initiale. Contrairement au cas d'un système défaillant, tout le matériel défectueux d'un système cible est remplacé.

système d'application

(terme propre à la sauvegarde ZDB) Système sur lequel s'exécute l'application ou la base de données. Les données de l'application ou de la base de données sont situées sur les volumes source.
Voir aussi système de sauvegarde et volume source.

système d'exploitation de récupération après sinistre

Voir DR OS.

système d'hébergement

Client Data Protector en fonctionnement utilisé pour la récupération après sinistre avec restitution de disque à l'aide d'un Agent de disque Data Protector installé.

système d'origine

Configuration système sauvegardée par Data Protector avant qu'un sinistre ne frappe le système.

Système de bibliothèques virtuelles (VLS)

Périphérique de stockage de données sur disque hébergeant une ou plusieurs bibliothèques de bandes virtuelles (VTL).

système de fichiers Organisation des fichiers sur un disque dur. Un système de fichiers est enregistré pour que les attributs et le contenu des fichiers soient stockés sur le support de sauvegarde.

Système de fichiers distribués (DFS) Service reliant les partages de fichiers dans un seul espace de noms. Ces partages peuvent résider sur le même ordinateur ou sur des ordinateurs différents. Le DFS permet à un client d'accéder aux ressources de manière transparente.

système de sauvegarde *(terme propre à la sauvegarde ZDB)* Système connecté à une baie de disques avec un ou plusieurs systèmes d'application. Le système de sauvegarde est généralement connecté à une baie de disques pour créer des volumes cibles (une réplique) et sert à monter les volumes cibles (la réplique).
Voir aussi système d'application, volume cible et réplique.

SysVol *(terme propre à Windows)* Répertoire partagé contenant la copie des fichiers publics du domaine sur le serveur. Ces fichiers sont reproduits sur tous les contrôleurs du domaine.

table des journaux de transactions *(terme propre à Sybase)* Table système où sont enregistrées automatiquement toutes les modifications apportées à la base de données.

thread *(terme propre à Microsoft SQL Server)* Entité exécutable appartenant à un seul processus. Elle comprend un compteur de programme, une pile en mode utilisateur, une pile en mode noyau et un ensemble de valeurs de registre. Plusieurs threads peuvent être exécutés en même temps dans un même processus.

TimeFinder *(terme propre à EMC Symmetrix)* Processus Business Continuance permettant de créer une copie instantanée d'un ou de plusieurs périphériques logiques Symmetrix (SLD). Cette copie est créée sur des SLD préconfigurés spécialement et appelés BCV ; elle est accessible via une adresse de périphérique distincte.

TLU Tape Library Unit ou unité de bibliothèque de bandes.

TNSNAMES.ORA *(terme propre à Oracle et SAP R/3)* Fichier de configuration réseau contenant des descripteurs de connexion mappés à des noms de services. Le fichier peut être géré au niveau central ou au niveau local afin d'être accessible à tous les clients ou à certains d'entre eux seulement.

transaction
Mécanisme destiné à s'assurer qu'un ensemble d'actions est considéré comme une seule unité de travail. Les bases de données utilisent les transactions pour effectuer un suivi des modifications.

type de support
Type physique d'un support, comme DDS ou DLT.

types de sauvegarde
Voir sauvegarde incrémentale, sauvegarde différentielle, sauvegarde de transaction, sauvegarde complète et sauvegarde delta.

UIProxy
Le serveur d'interface utilisateur graphique Java (le service `UIProxy`) s'exécute sur le Gestionnaire de cellule Data Protector. Il est chargé de la communication entre le client de l'interface Java et le Gestionnaire de cellule. De plus, il effectue des opérations logiques et envoie uniquement les informations importantes au client. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.

unité de commande principale (MCU, pour Main Control Unit)
(terme propre à HP P9000 XP Array Family) Unité HP StorageWorks P9000 XP Disk Array Family qui contient les volumes principaux (P-VOL) pour la configuration HP CA P9000 XP ou HP CA+BC P9000 XP et agit comme un périphérique maître.
Voir aussi HP Business Copy (BC) P9000 XP, HP Continuous Access (CA) P9000 XP et LDEV.

Unité de télécommande (RCU)
(terme propre à HP P9000 XP Array Family) Unité HP StorageWorks P9000 XP Disk Array Family qui sert de dispositif esclave pour l'unité de commande principale (MCU) dans la configuration HP CA P9000 XP ou HP CA + BC P9000 XP. Dans les configurations bidirectionnelles, la RCU peut également agir comme une MCU.

User Account Control (UAC)
Contrôle des comptes utilisateur - Composant de sécurité des systèmes d'exploitation Windows Vista, Windows 7 et Windows Server 2008 qui limite les logiciels d'application aux privilèges utilisateurs standard jusqu'à ce qu'un administrateur autorise une augmentation du niveau de privilèges.

vérification
Fonction permettant à l'utilisateur de contrôler si les données Data Protector stockées sur un support spécifique sont lisibles. En outre, si l'option CRC (contrôle de redondance cyclique) était

activée lors de la sauvegarde, vous pouvez contrôler la cohérence de chaque bloc.

vérification d'objet Processus consistant à vérifier l'intégrité des objets sauvegarde, du point de vue de Data Protector, et aptitude de Data Protector à les transmettre à la destination souhaitée. Ce processus peut servir à fournir un niveau de confiance en matière de capacité à restaurer des versions d'objets créées par des sessions de sauvegarde, de copie d'objet ou de consolidation d'objet.

version de fichier Un même fichier peut être sauvegardé plusieurs fois lors de sauvegardes complètes et incrémentales (si des modifications ont été apportées au fichier). Si le niveau de journalisation sélectionné pour la sauvegarde est TOUT, Data Protector conserve dans la base de données IDB une entrée pour le nom de fichier lui-même et une pour chaque version (date/heure) du fichier.

Virtual Controller Software (VCS) *(terme propre à HP P6000 EVA Array Family)* Micrologiciel gérant tous les aspects du fonctionnement du système de stockage, dont les communications avec HP StorageWorks Command View EVA via les contrôleurs HSV.
Voir aussi HP StorageWorks Command View (CV) EVA.

volser *(terme propre à ADIC et STK)* Un volser (VOLume SERial number - numéro de série de volume) est une étiquette située sur le support et servant à identifier la bande physique dans les très grandes bibliothèques. Il s'agit d'une appellation spécifique aux périphériques ADIC/GRAU et StorageTek.

volume cible *(terme propre à la sauvegarde ZDB)* Volume de stockage sur lequel les données sont répliquées.

volume de stockage *(terme propre à la sauvegarde ZDB)* Objet pouvant être présenté à un système d'exploitation ou à une autre entité (par exemple, un système de virtualisation) sur lequel existent des systèmes de gestion de volumes, des systèmes de fichiers ou d'autres objets. Les systèmes de gestion de volumes et les systèmes de fichiers sont basés sur ce type de stockage. Habituellement, ils peuvent être créés ou existent déjà dans un système de stockage tel qu'une baie de disques.

volume principal (P-VOL) *(terme propre à HP P9000 XP Array Family)* Disque interne (LDEV) d'une baie de disques HP StorageWorks P9000 XP Disk

Array Family pour lequel il existe un volume secondaire (S-VOL) : son miroir ou un volume à utiliser pour le stockage des snapshots. Dans les configurations HP CA P9000 XP et HP CA + BC P9000 XP, les volumes principaux sont situés dans l'unité de commande principale (MCU).
Voir aussi volume secondaire (S-VOL) et unité de commande principale (MCU).

volume secondaire (S-VOL) *(terme propre à HP P9000 XP Array Family)* Disque interne (LDEV) dune baie de disques HP StorageWorks P9000 XP Disk Array Family qui est apparié à un autre LDEV : un volume principal (P-VOL). Il peut jouer le rôle de miroir du P-VOL ou servir de volume de stockage pour le snapshot du P-VOL. Une adresse SCSI différente de celle utilisée pour le P-VOL est affectée au S-VOL. Dans une configuration HP CA P9000 XP, les S-VOL qui servent de miroirs peuvent être utilisés comme périphériques de secours dans une configuration MetroCluster.
Voir aussi volume principal (P-VOL) et unité de commande principale (MCU).

Volume Shadow Copy Service *Voir* Microsoft Volume Shadow Copy Service (VSS).

volume source *(terme propre à la sauvegarde ZDB)* Volume de stockage contenant les données à répliquer.

volume/disque/partition d'amorçage Volume/disque/partition contenant les fichiers nécessaires à la première étape du processus d'amorçage. La terminologie utilisée par Microsoft définit le volume/disque/partition d'amorçage comme le volume/disque/partition contenant les fichiers du système d'exploitation.

volume/disque/partition système Volume/disque/partition contenant les fichiers du système d'exploitation. La terminologie utilisée par Microsoft définit ces éléments comme ceux contenant les fichiers nécessaires pour assurer les premières étapes du processus d'amorçage.

VSS *Voir* Microsoft Volume Shadow Copy Service (VSS).

VxFS Veritas Journal Filesystem, système de fichiers journaux Veritas.

VxVM (Veritas Volume Manager) Le VVM (Veritas Volume Manager), ou Gestionnaire de volume Veritas, est un système permettant de gérer l'espace disque sur les plates-formes Solaris. Un système VxVM est constitué de

groupes arbitraires d'un ou plusieurs volumes physiques organisés en groupes de disques logiques.

Wake ONLAN Support de mise en marche distant pour les systèmes s'exécutant en mode d'économie d'énergie à partir d'un autre système du même réseau local.

ZDB *Voir* sauvegarde avec temps d'indisponibilité nul (ZDB).

zone de récupération flash *(terme propre à Oracle)* Groupe de disques de gestion de stockage automatique, de système de fichiers ou de répertoires gérés par Oracle qui sert de zone de stockage centralisé pour des fichiers liés à la sauvegarde, la restauration et la récupération de base de données (fichiers de récupération). *Voir aussi* fichiers de récupération.

Index

B

C

D

E

F

G

H

I

J

N

O

P

R

S

T

U

V

W