Data Protector

Version du logiciel : 10.00

Guide d'installation

Date de publication du document : Juin 2017
Date de lancement du logiciel : Juin 2017

Informations légales

Garantie

Les seules garanties applicables aux produits et services Micro Focus or one of its affiliates sont celles figurant dans les déclarations de garantie expresse accompagnant les dits produits et services. Aucun terme de ce document ne peut être interprété comme constituant une garantie supplémentaire. Micro Focus ne peut en aucun cas être tenu pour responsable des erreurs ou omissions techniques ou rédactionnelles du présent document.

Les informations contenues dans le présent document peuvent être modifiées sans préavis.

Légende de droits réservés

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

Copyright

Marques

Adobe™ est une marque de commerce de Adobe Systems Incorporated.

Microsoft® et Windows® sont des marques déposées de Microsoft Corporation.

UNIX® est une marque déposée de The Open Group.

Ce produit inclut une interface de la bibliothèque de compression d'intérêt général 'zlib', qui est sous Copyright © 1995-2002 Jean-loup Gailly et Mark Adler.

Mises à jour de la documentation

La page de titre de ce document comprend les informations d'identification suivantes :

- Numéro de version du logiciel, qui indique la version logicielle.
- Date de publication du document, qui est modifiée après chaque mise à jour du document.
- Date de publication du logiciel, qui indique la date de publication de cette version du logiciel.

Pour vérifier les récentes mises à jour logicielles, accédez à la page : https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=patches?keyword=.

Pour vérifier que vous disposez de l'édition la plus récente d'un document, accédez à la page : https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.

Pour accéder à ce site, vous devez créer un compte Passport et vous connecter. Pour obtenir un identifiant Passport, accédez à l'adresse : https://cf.passport.softwaregrp.com/hppcf/login.do.

Vous recevrez également des mises à jour et les nouvelles versions si vous inscrivez au service de support produit approprié. Pour plus d'informations, contactez votre revendeur.

Support

Visitez le site d'assistanceSoftware à l'adresse : https://softwaresupport.softwaregrp.com/

Ce site fournit les informations de contact et les détails sur les offres de produits, de services et d'assistance Software.

L'assistance en ligne de Software propose des fonctions de résolution autonome. Le site constitue un moyen efficace d'accéder aux outils interactifs d'assistance technique nécessaires à la gestion de votre activité. En tant que client privilégié de l'assistance, vous pouvez depuis ce site :

- Rechercher des documents appropriés
- Envoyer et suivre des cas de support et des demandes d'amélioration
- Télécharger des correctifs logiciels
- Accéder à la documentation produit
- Gérer des contrats de support
- Rechercher des contacts de l'assistance clientèle
- Consulter des informations sur les services disponibles
- Discuter avec d'autres utilisateurs de logiciels
- Rechercher des formations logicielles et vous y inscrire

Pour accéder à la plupart des offres d'assistance, vous devez vous enregistrer en tant qu'utilisateur disposant d'un compte Passport et vous identifier comme tel. De nombreuses offres nécessitent en outre un contrat d'assistance.

Pour obtenir un identifiant Passport, accédez à l'adresse https://cf.passport.softwaregrp.com/hppcf/login.do.

Pour plus d'informations sur les niveaux d'accès, accédez à la page : https://softwaresupport.softwaregrp.com/.

Sommaire

Chapitre 1: Présentation de la procédure d'installation

Ce chapitre fourni une présentation de la procédure d'installation de Data Protector et introduit des concepts qui s'appliquent à l'installation. Ce chapitre introduit également les interfaces utilisateur du Gestionnaire de cellule de Data Protector et de Data Protector.

Présentation de la procédure d'installation

Un environnement de sauvegarde Data Protector est un semble de systèmes possédant une stratégie de sauvegarde commune, situés dans le même fuseau horaire et existant sur un même LAN/SAN. Cet environnement réseau est désigné par le terme de Data Protector**cellule**. Une cellule typique comprend un Gestionnaire de cellule, des Serveur d'installation, des clients, et des périphériques de sauvegarde.

Le Gestionnaire de cellule est le système principal en charge de centraliser la gestion de la cellule. Il contient la Base de données interne (IDB) de Data Protector et fait tourner le client Data Protector central et les gestionnaires de session.

L'IDB garde une trace des fichiers sauvegardés et de la configuration des cellules.

Le **Serveur d'installation** est un système séparé ou un composant Gestionnaire de cellule qui contient le référentiel du client Data Protector utilisé pour les installations à distance des clients. Cette fonctionnalité de Data Protector facilite grandement le processus d'installation des logiciels, particulièrement pour les clients à distance.

Une cellule typique est constituée d'un Gestionnaire de cellule et de plusieurs clients. Un système informatique devient un Data Protector **client** dès qu'un des composants logiciel Data Protector est installé sur le système. Les composants client installés sur un système dépendent du rôle de ce système dans votre environnement de sauvegarde. Les composants Data Protector peuvent être installés soit en local sur un seul système, soit sur plusieurs systèmes à partir des Serveur d'installation.

Le composant **Interface utilisateur** de est nécessaire pour accéder aux fonctionnalités de Data Protector et est utilisé pour effectuer toutes les tâches de configuration et d'administration. Il doit être installé sur les systèmes utilisés pour l'administration des sauvegardes. Data Protector fournit une interface graphique (GUI) et une interface en ligne de commande (CLI).

Des composants Data Protector **Agent de disque** adéquats doivent être installés sur les systèmes client avec disques qui ont besoin d'être sauvegardés. L'Agent de disque vous permet de sauvegarder les données issues du disque client ou de les restaurer.

Des composants agent d'intégration Data Protector adéquat doivent être installés sur les systèmes client avec applications et environnements virtuels qui ont besoin d'être sauvegardés. L'Agent d'intégration vous permet de sauvegarder les données issues d'une application ou d'un environnement virtuel, ou de les restaurer.

Un composant **Agent de support** soit être installé sur les systèmes client connectés à un périphérique de sauvegarde. Ce logiciel gère les périphériques de sauvegarde et de support. Data Protector contient deux Agents de support : l'**Agent de support général** et l'**Agent de support NDMP**. L'Agent de support NDMP n'est nécessaire que sur les systèmes client qui contrôlent la sauvegarde d'un serveur NDMP (sur des

systèmes client qui contrôlent des lecteurs dédiés NDMP). Dans tous les autres cas, les deux Agents de support sont interchangeables.

Avant d'installer Data Protector sur votre réseau, établissez :

- Le système sur lequel le Gestionnaire de cellule sera installé. Pour voir les systèmes d'exploitation et les versions pris en charge, consultez les dernières matrices de support à l'adresse suivante : https://softwaresupport.softwaregrp.com/.

  Il ne peut y avoir qu'un seul Gestionnaire de cellule par cellule. Data Protector ne peut fonctionner sans Gestionnaire de cellule installé.
- Les systèmes qui seront utilisés pour accéder aux fonctionnalités de Data Protector grâce à l'interface utilisateur. Un composant Interface utilisateur doit être installé sur ces systèmes.
- Les systèmes qui seront sauvegardés. Ils doivent disposer du composant Agent de disque installé pour pouvoir sauvegarder le système de fichier et du composant agent d'application correspondant pour intégrer la base de données en ligne.
- Les systèmes sur lesquels les périphériques de sauvegarde seront connectés. Ils doivent avoir le composant Agent de support installé.
- Un ou plusieurs systèmes sur lesquels le Data Protector Serveur d'installation sera installé. Deux types de Serveur d'installation sont disponibles pour une installation de logiciel à distance : un pour les clients UNIX, et un pour les clients Windows.

  Le choix de système pour le Serveur d'installation est indépendant du Gestionnaire de cellule et des systèmes sur lesquels l'Interface utilisateur est installée. Le Gestionnaire de cellule et le Serveur d'installation peuvent être installés sur le même système ou sur des systèmes différents.

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

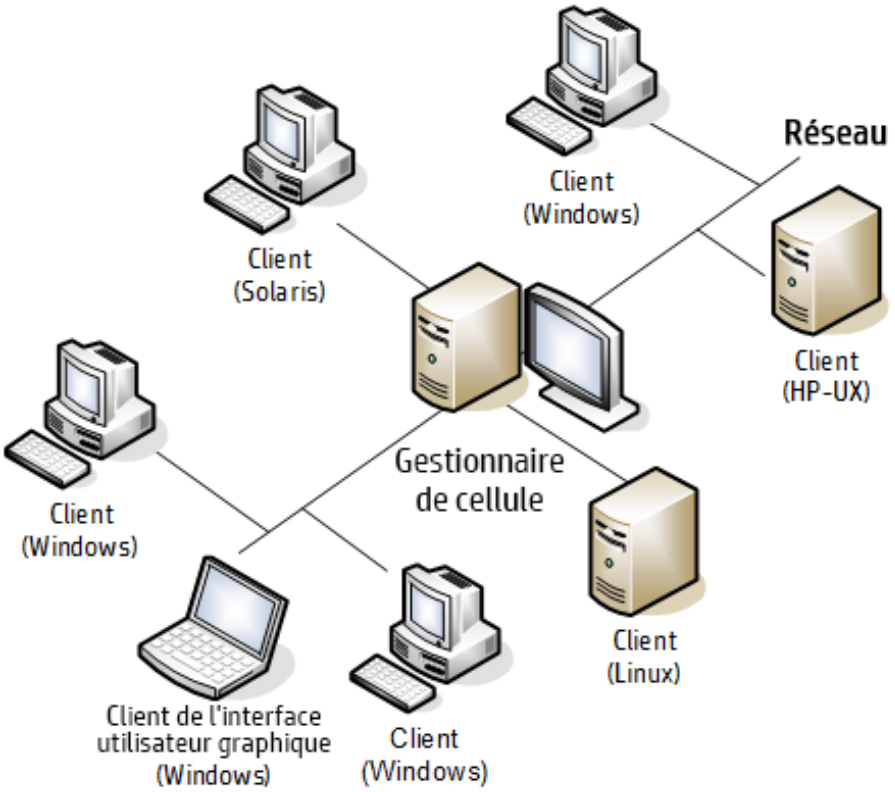
> **IMPORTANT :**
> Lors de l'installation d'un client Data Protector sur des systèmes Solaris, assurez-vous de sauvegarder dans un autre répertoire tous vos fichiers situés dans le répertoire `/usr/omni` . L'installation de Data Protector supprimera tous les fichiers du répertoire `/usr/omni`.

Une fois les rôles des systèmes de votre future cellule Data Protector définis, la procédure d'installation comprend les étapes suivantes :

1. Vérification des spécifications en vue de l'installation.
2. Installation du Data Protector Gestionnaire de cellule.
3. Installation du ou des Serveur d'installation et de l'interface utilisateur.
4. Installation des systèmes client soit à distance (option recommandée quand c'est possible), soit en local avec le package d'installation (zip/tar).

> **REMARQUE :**
> Vous ne pouvez installer à distance un client Data Protector sur un système Windows si un Serveur d'installation a déjà été installé sur le système. Pour installer un Serveur d'installation ou des composants client sur le même système, vous devez effectuer une installation du client en local à partir du package d'installation en zip de Data Protector pour Windows. Dans la fenêtre Installation personnalisée, sélectionnez tous les composants client voulus et le composant Serveur d'installation.
>
> L'installation à distance est également impossible pour l'Édition familiale de Windows XP et pour les clients HP OpenVMS. Ces cas demandent une installation en local.

Cellule Data Protector



Concept de l'installation à distance

Chaque fois que vous effectuez une installation à distance, vous accédez au Serveur d'installation via l'interface graphique. Le composant Interface utilisateur peut être installé sur le Gestionnaire de cellule, bien que ça ne soit pas une obligation. Il peut être prudent d'installer l'Interface utilisateur sur plusieurs systèmes pour pouvoir accéder au Gestionnaire de cellule de plusieurs endroits.

Le logiciel client peut être distribué à n'importe quel système Windows depuis un Serveur d'installation pour Windows.

Les systèmes Windows doivent être installés en local avec le package d'installation Windows Data Protector en zip.

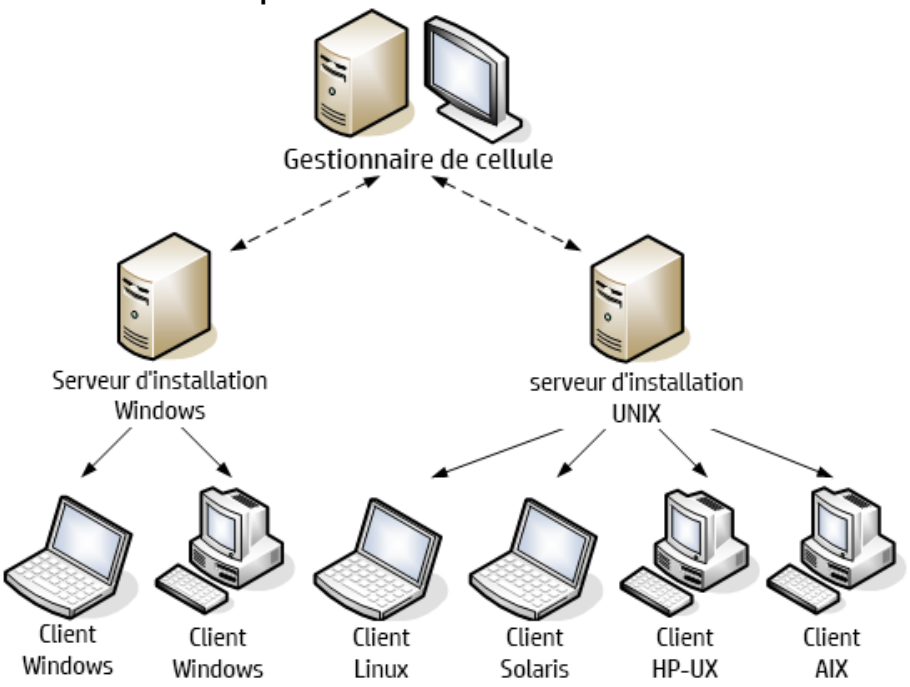
Le logiciel client peut être installé à distance sur HP-UX, Solaris, Linux, AIX, et tout autre système d'exploitation UNIX pris en charge, depuis un Serveur d'installation pour systèmes UNIX. Pour obtenir une liste des plates-formes prises en charge, voir. *Data ProtectorMatrices de prise en charge*. Bien qu'un Serveur d'installation ne soit pas requis pour l'installation de clients en local, il est requis pour mettre à jour les clients.

Pour les systèmes d'exploitation UNIX qui ne prennent pas en charge l'installation à distance, ou si vous n'installez pas de Serveur d'installation pour UNIX, il est possible d'installer les clients UNIX en local depuis le package d'installation tar de Data Protector pour UNIX.

Pour plus d'informations sur les méthodes d'installation disponibles pour les différents clients Data Protector, reportez-vous à Installer des clients Data Protector, Page 54.

Pour obtenir la procédure de désinstallation locale des clients UNIX, reportez-vous à Installation locale sur les systèmes UNIX et Mac OS X, Page 103.

Data ProtectorConcept d'une installation de



Supports d'installation de Data Protector

Data Protector prend en charge différents systèmes d'exploitation et plusieurs architectures de processeur. Le logiciel est fourni sous forme de package zip/tar.

> **REMARQUE :**
> Les fichiers d'installation de Data Protector pour les systèmes Windows Server 2008 et Windows Server 2012 disposent de la signature digitale de Micro Focus.

Le tableau ci-dessous liste les différents packages disponibles au téléchargement à l'adresse https://softwaresupport.softwaregrp.com/.

Nom du package	Sommaire
Logiciel Data Protector 10.00 Windows `DP_A1000_Windows_OVMS.zip`	• Gestionnaire de cellule et Serveur d'installation pour systèmes Windows 64-bit (AMD64/Intel EM64T) • Intégralité des guides en anglais et localisés au format électronique PDF. • Clients Windows 32/64-bit • Clients HP OpenVMS (systèmes Alpha et Itanium) • Information produit • Packages d'intégration logicielle

Nom du package	Sommaire
Client Data Protector 10.00 HP-UX `DP_A1000_UX11x.tar.gz`	• Gestionnaire de cellule, Serveur d'installation, et clients pour systèmes HP-UX • Clients pour autres systèmes UNIX • Clients pour systèmes Mac OS X • Intégralité des guides en anglais et localisés au format électronique PDF. • Packages d'intégration logicielle
Client Data Protector 10.00 Linux `DP_A1000_GPLx86_64.tar.gz`	• Gestionnaire de cellule, Serveur d'installation, et clients pour systèmes Linux • Clients pour autres systèmes UNIX • Clients pour systèmes Mac OS X • Intégralité des guides en anglais et localisés au format électronique PDF. • Packages d'intégration logicielle

Choisir le système du Gestionnaire de cellule

Le Gestionnaire de cellule est le système principal de la cellule Data Protector. Il centralise la gestion de la cellule. Le Gestionnaire de cellule possède les fonctions suivantes :

- Lancer le client central de Data Protector.
- Héberger le serveur de la base de données interne (IDB) de Data Protector.
- Collecter et maintenir les données contenant les informations sur les sessions Data Protector.
- Lancer les Gestionnaires de session qui démarrent et arrêtent différents types de sessions Data Protector et stockent les informations qui y sont associées dans l'IDB.

Avant de décider du système de votre environnement qui recevra l'installation du Gestionnaire de cellule, soyez conscient des éléments suivants :

- Plateformes prises en charge

  Le Gestionnaire de cellule peut être installé sur des plateformes Windows, HP-UX, ou Linux.

  Pour plus de détails sur les versions et les sous versions prises en charge pour ces plateformes, consultez les dernières matrices de support à l'adresse suivante : https://softwaresupport.softwaregrp.com/.
- Fiabilité du système Gestionnaire de cellule

  Étant donné que le Gestionnaire de cellule contient l'IDB et que la sauvegarde et la restauration ne peuvent être effectuées si le Gestionnaire de cellule ne fonctionne pas correctement, il est important de choisir un système fiable de votre environnement pour l'installation.
- Croissance de la base de données et espace disque requis

  Le Gestionnaire de cellule garde la base de données interne (IDB) de Data Protector. L'IDB contient les informations sur les données sauvegardées et leurs supports, les messages de session et les

périphériques. L'IDB peut grossir jusqu'à atteindre une taille conséquente, en fonction de votre environnement. Par exemple, si la majorité de vos sauvegardes sont des sauvegardes de systèmes de fichiers, alors une taille normale pour l'IDB représenterait 2% de l'espace disque utilisé par les données sauvegardées.

Pour plus d'informations sur la planification et la gestion de la taille et de la croissance de la base de données, vous pouvez vous reportez à l'index *Aide de Data Protector* : «croissance et performances de l'IDB».

Pour les exigences en matière d'espace libre disque minimum pour l'IDB, consultez le Annonces sur les produits, notes sur les logiciels et références Data Protector.

> **REMARQUE :**
> Vous n'avez pas besoin d'utiliser le Gestionnaire de cellule comme système pour l'interface utilisateur. Par exemple, vous pouvez avoir votre Gestionnaire de cellule installé sur un système UNIX et votre interface utilisateur de Data Protector installée sur un système possédant une plateforme sous Windows..

Étapes suivantes

Pour déterminer les exigences minimales pour votre système futur Gestionnaire de cellule, voir Installation du Gestionnaire de cellule et des Serveur d'installationde Data Protector, Page 26.

Choisir le système de l'interface utilisateur de Data Protector

Data Protector fournit deux interfaces utilisateur : une interface graphique (GUI) et une interface de ligne en commande (CLI). L'interface graphique est disponible pour les plateformes Windows, et l'interface de ligne en commande est disponible pour les plateformes Windows, HP-UX, Solaris, et Linux. Chaque interface est fournie et installée en tant que composant logiciel solo de Data Protector.

Le système choisi pour contrôler la cellule sera utilisé par un administrateur réseau ou un opérateur de sauvegarde. Cependant, dans un grand environnement informatique, il peut être intéressant d'avoir une interface utilisateur sur plusieurs systèmes, et même sur plusieurs plateformes dans le cas d'un environnement hétérogène.

Pour plus de détails sur les systèmes d'exploitation pris en charge (versions, sous versions, éditions) pour l'interface utilisateur, consultez les dernières matrices de prise en charge disponibles à l'adresse suivante : https://softwaresupport.softwaregrp.com/. Pour plus d'information sur la prise en charge des langues locales et l'utilisation de caractères non -ASCII dans les noms de fichier, reportez-vous à l'index de *Aide de Data Protector* : «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 depuis ce système. Vous n'avez pas besoin d'utiliser le système de l'interface graphique sur le Gestionnaire de cellule.

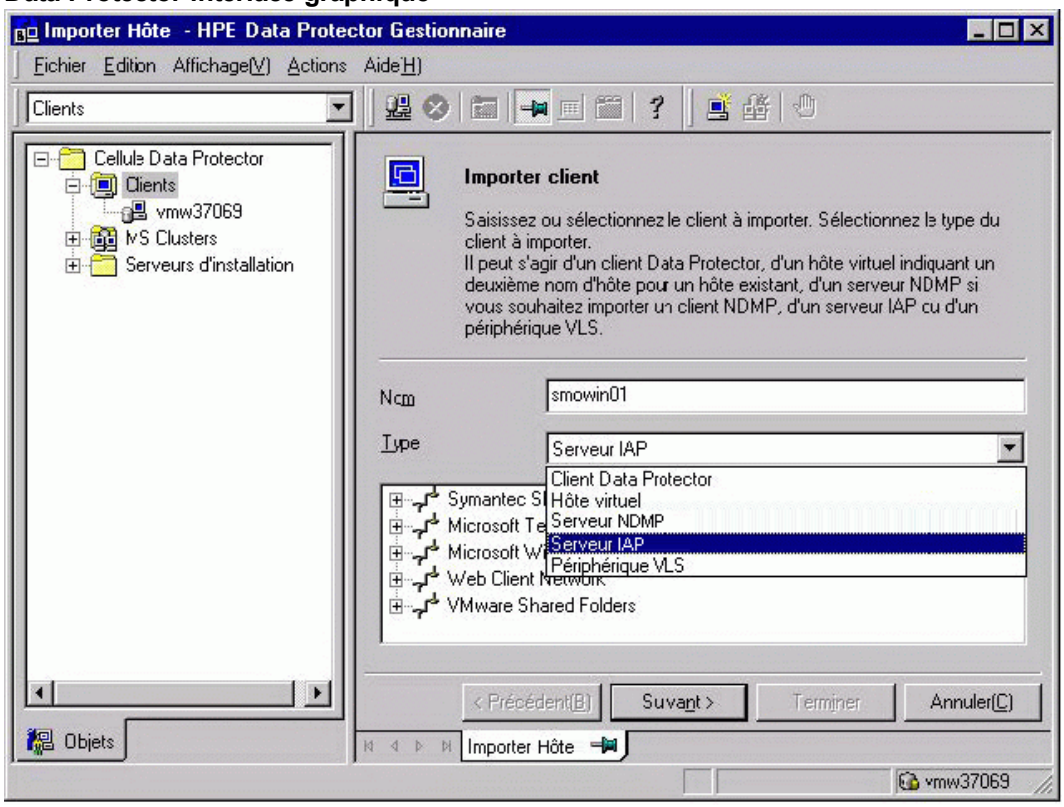
L'interface graphique de Data Protector

L'interface graphique de Data Protector est une puissante interface utilisateur qui permet un accès facile aux fonctionnalités de Data Protector. La fenêtre principale contient plusieurs affichages, comme

Clients, **Utilisateurs**, **Périphériques & Supports**, **Sauvegarder**, **Restaurer**, **Opérations sur les objets**, **Rapports**, **Écran de contrôle**, **Récupération instantanée**, et **Base de données interne**, qui vous permettent d'effectuer toutes les tâches correspondantes.

Par exemple, dans l'affichage **Clients**, vous pouvez installer (ajouter) des clients à distance en spécifiant tous les systèmes cibles et en définissant les chemins d'installation et les options envoyées au Serveur d'installation spécifié. Une fois l'installation du client lancée, seuls les messages propres à l'installation sont affichés sur la fenêtre de l'écran de contrôle.

Data Protector interface graphique



Voir également Interface graphique de Data Protector, Page 402 qui décrit les éléments les plus importants de l'interface graphique de Data Protector.

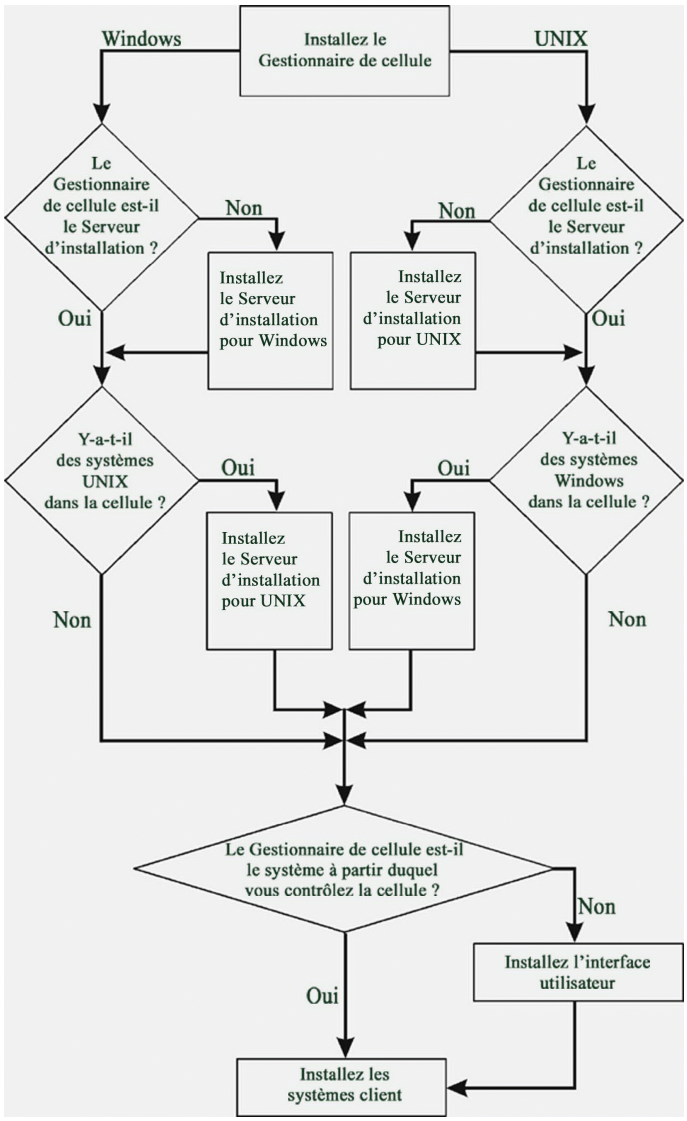
Chapitre 2: Installation de Data Protector

Ce chapitre contient les instructions détaillées concernant :

- L'installation du Data Protector et des Gestionnaire de cellule de Serveur d'installation
- L'installation de Data Protector Single Server Edition

Installation du Gestionnaire de cellule et des Serveur d'installationde Data Protector

procédure d'installation



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

IMPORTANT :
Tous les fichiers de configuration et d'information de session d'une cellule Data Protector sont stockées sur le Gestionnaire de cellule. Il est difficile de transférer cette information sur un autre système. C'est pourquoi il est important de s'assurer que le Gestionnaire de cellule soit un système fiable dans un environnement stable et contrôlé.

REMARQUE :
Les précédentes versions de l'interface graphique Data Protector 10.00 ne sont pas compatibles avec Data Protector 10.00 Gestionnaire de cellule.

Installing a UNIX Gestionnaire de cellule

Cette section fournit les instructions étape par étape pour installer un Gestionnaire de cellule pour UNIX. Pour installer uniquement le Gestionnaire de cellule Windows, voir Installing a Windows Gestionnaire de cellule, Page 34.

Conditions préalables

- Une recherche DNS indirecte pour résoudre le nom d'hôte est requise pour tous les composants Data Protector de la cellule Data Protector.
- Les utilisateurs par défaut `unmask` doivent être définis sur `022`, faute de quoi certains services de Data Protector risquent de ne pas démarrer.
- Le compte utilisateur utilisé pour l'installation doit avoir les privilèges d'administratifs (`root`) sur le système cible sélectionné.
- Le système qui deviendra le Gestionnaire de cellule doit :
  - Posséder un système d'exploitation UNIX pris en charge installé. Pour avoir la liste des systèmes d'exploitation pris en charge pour le Gestionnaire de cellule, reportez-vous à https://softwaresupport.softwaregrp.com/.
  - Avoir suffisamment d'espace disque disponible pour le logiciel de Data Protector Gestionnaire de cellule. Le Gestionnaire de cellule doit avoir les spécificités suivantes :
    - La Limite souple de fichiers par processus du Gestionnaire de cellule doit être au moins 1024.
    - ***Systèmes HP-UX :*** 8 GB de RAM totale ; ***Systèmes Linux :*** 4 GB de RAM totale

    Pour chaque session de sauvegarde parallèle, 40 MB de RAM et entre 5 et 8 MB par taille de segment de données sont demandées. Par exemple, si vous voulez effectuer 60 sessions de sauvegarde parallèles, 3 GB de RAM plus 512 MB pour les segments de données sont nécessaires.

    Vous pouvez passer outre le manque d'espace disque disponible en installant Data Protector dans des répertoires liés. Avant de créer les liens, consultez Structure des répertoires installés sur systèmes HP-UX et Linux, Page 30.
  - Disposer d'un espace disque suffisant pour la base de données interne (IDB) Data Protector.

Pour la restauration de la base de données interne, le double de RAM totale est requis. Avoir 1,5 GB d'espace disque disponible et environ 100 bytes pour chaque fichier sauvegardé (pour être utilisé par l'IDB) dans le répertoire /var, où l'IDB est stockée. Notez que le fonctionnement actuel de l'IDB permet de déplacer les fichiers binaires de la base de données si cela devient nécessaire à cause de la croissance de sa taille.

Si l'espace de stockage disponible est insuffisant sur le volume de disque, vous pouvez utiliser des répertoires associés, mais nous vous conseillons de créer les liens avant l'installation et de vérifier que les répertoires de destination existent.

- Disposer du protocole TCP/IP installé et en exécution. Ce protocole doit pouvoir résoudre les noms d'hôte.
- Reconnaitre le système du Gestionnaire de cellule si un serveur NIS est utilisé. Voir Préparation d'un serveur NIS, Page 358.
- Avoir les ports suivants disponibles :
  - 5565 — port requis pour une nouvelle installation dans Data Protector.
  - 5555 — port requis pour la mise à niveau de l'installation de Data Protector.
  - 7112 — port de service de la base de données interne
  - 7113 — port du pooler des connexions de la base de données interne (IDB CP)
  - 7116 — port du serveur d'application (HTTPS AS)
  - 9999 — port de gestion du serveur d'application

  Pour changer le numéro du port de communication par défaut, consultez le Changer le port Inet par défaut Data Protector, Page 354.
  Pour modifier les ports IDB et du serveur d'application par défaut, consultez Changer les ports IDB et les comptes utilisateurs par défaut de Data Protector sur des systèmes UNIX, Page 355.
- Prendre en charge les noms de fichier longs. Pour vérifier si votre système de fichier prend en charge les noms de fichier longs, exécutez la commande `getconf NAME_MAX DirectoryPath`.
- La calculatrice en ligne de commande Basic (bc) doit être installée.
- Avoir le groupe utilisateur `hpdp` et le compte utilisateur dédié `hpdp` dans ce groupe d'utilisateurs configuré pour être utilisé par Data Protector. Pour changer le compte utilisateur par défaut, consultez Changer les ports IDB et les comptes utilisateurs par défaut de Data Protector sur des systèmes UNIX, Page 355.
- Avoir le dossier de base par défaut configuré pour l'utilisateur hpdp, sans quoi certains des services de Data Protector pourraient ne pas se lancer au démarrage.
- L'utilisateur `hpdp` doit avoir accès à tous les répertoires depuis les chemins suivants, qui existent déjà dans le système :
  - `/opt/omni/*`
  - `/etc/opt/omni/*`
  - `/var/opt/omni/*`

Systèmes Linux :

- La bibliothèque 32-bit GNU C (glibc) doit être installée sur les systèmes Linux 64-bit (x86_64).
- Les net-tools doivent être installés (certains utilitaires net-tools sont nécessaires au cours de l'installation).

Gestionnaire de cellule compatible cluster

Des conditions préalables et des étapes supplémentaires sont nécessaires pour l'installation d'un Gestionnaire de cellule compatible cluster. Voir Installation d'un Gestionnaire de cellule compatible cluster, Page 166.

> **REMARQUE :**
> Dans un environnement à multiples cellules (MoM), tous les Gestionnaire de cellule doivent avoir la même version de Data Protector installée.

Recommandations

- Micro Focus recommande l'usage de la prise en charge de gros fichiers (LFS) sur les systèmes de fichiers chargés de stocker la base de données interne et les fichiers binaires DC de Data Protector qui devraient finir par dépasser les 2 GB.

Configurer les paramètres du noyau

Systèmes HP-UX :

- Définissez le paramètre de noyau `shmmax` (taille maximale d'un segment de mémoire partagé) sur au moins 2,5 Go. Pour vérifier la configuration, exécutez :

  ```
  kcusage shmmax
  ```

- Micro Focus recommande un paramètre de noyau `maxdsiz` (taille maximale d'un segment de mémoire) ou `maxdsiz_64` à 134217728 bytes minimum (128 Mo) et un paramètre de noyau `semmnu` (nombre de structures Défaire sémaphores) à 4000 minimum. Le paramètre `semmnu` doit permettre un nombre maximal de sauvegardes en parallèle ou de sessions de restauration ou de copie (1000) et le même nombre de sessions d'interrogations de base de données (1000). Il est inutile de modifier la valeur du paramètre `semmnu` si vous n'envisagez pas de lancer un grand nombre de sessions parallèles.

  Après avoir validé ces changements, redémarrez le système.

Systèmes Linux :

- Définissez le paramètre de noyau `shmmax` (taille maximale d'un segment de mémoire partagé) sur au moins 2,5 Go. Pour vérifier la configuration, exécutez :

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

  Pour la récupération de la base de données interne, le paramètre de noyau doit être mis au moins au double de la valeur indiquée ci-dessus.

Procédure d'installation

Si vous installez Gestionnaire de cellule et Serveur d'installation sur le même système, vous pouvez exécuter `omnisetup.sh -CM -IS` pour faire l'installation en une seule étape.

Pour une description de la commande `omnisetup.sh`, consultez le fichier `README` disponible dans le package tar, ou le *Guide de référence de l'interface de ligne de commande Data Protector* situé dans le répertoire `/DOCS/C/MAN` du package tar.

Pour installer le Gestionnaire de cellule sur un système HP-UX ou Linux

1. Copiez le package d'installation Data Protector téléchargé (tar) sur le système HP-UX ou Linux et extrayez les fichiers vers un répertoire local.

   `LOCAL_INSTALL`

   `platform_dir` `/DP_DEPOT`

   Où *rép_plateforme* est :

`hpux`	pour les systèmes HP-UX
`linux_x86_64`	pour les systèmes Linux

2. Allez dans le répertoire `LOCAL_INSTALL` et exécutez :

   `./omnisetup.sh -CM`

   Pour plus d'informations sur la commande `omnisetup.sh`, reportez-vous au document *Guide de référence de l'interface de ligne de commande Data Protector*.

Si vous désirez installer un Serveur d'installation pour UNIX sur votre Gestionnaire de cellule, vous pouvez le faire à ce moment-là. Pour connaître la procédure, voir Installer des Serveur d'installation pour systèmes UNIX, Page 42.

Structure des répertoires installés sur systèmes HP-UX et Linux

Une fois l'installation terminée, le client central de Data Protector est situé dans le répertoire et le `/opt/omni/bin`Serveur d'installation pour UNIX se trouve dans le répertoire `/opt/omni/databases/vendor`. La liste suivante montre les sous répertoires de Data Protector et leur contenu :

> **IMPORTANT :**
> Pour installer Data Protector dans des répertoires liés, par exemple :
>
> `/opt/omni/ -> /prefix/opt/omni/`
>
> `/var/opt/omni/ -> /prefix/var/opt/omni/`
>
> `/etc/opt/omni/ -> /prefix/etc/opt/omni/`
>
> il est recommandé de créer les liens avant l'installation et de s'assurer que les répertoires de destination existent.

/opt/omni/bin	Commandes utilisateur
/opt/omni/help/C	Aide
/opt/omni/lbin	Commandes administratives, outils en ligne de commande
/opt/omni/sbin	Commandes administratives, outils en ligne de commande
/opt/omni/sbin/install	Scripts d'installation
/etc/opt/omni	Données de configuration
/opt/omni/lib	Bibliothèques partagées pour la compression, l'encodage de données et la manipulation de périphérique
/opt/omni/doc/C	Guides au format PDF.
/var/opt/omni/log /var/opt/omni/server/log	Fichiers journaux
/opt/omni/lib/nls/C	Fichiers catalogues de messages
/opt/omni/lib/man	Manuels
/var/opt/omni/tmp	Fichiers temporaires
/var/opt/omni/server/db80	Fichiers IDB Pour plus de détails, consultez l'index de *Aide de Data Protector* : "IDB, emplacement des répertoires".
/opt/omni/AppServer	Serveur d'application Data Protector.
/opt/omni/idb	Base de données interne Data Protector.
/opt/omni/jre	Environnement JRE à utiliser avec Data Protector

Configurer le démarrage et l'arrêt automatique

La procédure d'installation de Data Protector configure un démarrage et un arrêt automatique de tous les processus Data Protector dès qu'un système redémarre. Certaines parties de cette configuration sont dépendantes du système d'exploitation.

Les fichiers suivants sont automatiquement configurés :

Systèmes HP-UX :

/sbin/init.d/omni	Un script avec des procédures de démarrage et de fermeture.
/sbin/rc1.d/K162omni	Un lien vers le script /sbin/init.d/omni qui arrête Data Protector.
/sbin/rc2.d/S838omni	Un lien vers le script /sbin/init.d/omni qui démarre Data Protector.
/etc/rc.config.d/omni	Contient un paramètre omni défini comme suit :

	`omni=1` Data Protector est automatiquement arrêté ou démarré au redémarrage du système. Il s'agit de l'option par défaut. `omni=0` Data Protector n'est pas automatiquement arrêté ou démarré au redémarrage du système.

Systèmes Linux :

`/etc/init.d/omni`	Un script avec des procédures de démarrage et de fermeture.
`/etc/rc`*`init_level`*`.d/K10omni`	Un lien vers le script `/etc/init.d/omni` qui arrête Data Protector. Où *niv_init* est 1 et 6.
`/etc/rc`*`init_level`*`.d/S90omni`	Un lien vers le script `/etc/init.d/omni` qui démarre Data Protector. Où *niv_init* est 2,3,4 et 5.

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

Systèmes HP-UX :

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

Quand l'installation est terminée, les processus suivants sont lancés sur le Gestionnaire de cellule :

`/opt/omni/lbin/crs`	Le service Data Protector `Cell Request Server (CRS)` s'exécute sur le système du Gestionnaire de cellule et démarre lorsque le logiciel Gestionnaire de cellule est installé sur le système. Le CRS démarre et contrôle les sessions de sauvegarde et de restauration de la cellule.
`/opt/omni/lbin/mmd`	Le service Data Protector `Media Management Daemon (MMD)` s'exécute sur le système du Gestionnaire de cellule et démarre lorsque le logiciel Gestionnaire de cellule est installé sur le système. Le MMD gère les opérations de gestion de périphérique et de support.
`/opt/omni/lbin/kms`	Le service Data Protector `Key Management Server (KMS)` s'exécute sur le système du Gestionnaire de cellule et démarre lorsque le logiciel Gestionnaire de cellule est installé sur le système. Ce service gère les clés pour la fonction de cryptage de Data Protector.

/opt/omni/idb/bin/postgres	Le service Data Protector Internal Database Service (hpdp-idb) est celui sous lequel s'exécute la base de données IDB. Le service est accédé localement sur le Gestionnaire de cellule par les processus qui ont besoin d'informations issues de la base de données interne. Ce service est accédé à distance uniquement pour les informations de gestion des supports sur le point d'être transférées de l'IDB du Gestionnaire de cellule vers l'IDB du Manager-of-Manager (MoM).
/opt/omni/idb/bin/pgbouncer	Le service Data Protector Internal Database Connection Pooler (hpdp-idb-cp) propose un pool de connexions ouvertes à hpdb-idb qui peuvent être utilisées à la demande au lieu d'ouvrir une nouvelle connexion pour chaque requête, ce qui permet d'assurer l'extensibilité de la connexion hpdb-idb. Le service tourne sur le Gestionnaire de cellule et ne peut être accédé que par des processus locaux.
/opt/omni/AppServer/bin/standalone.sh	Le service Data Protector Application Server (hpdp-as) est utilisé pour la connexion de l'interface graphique à l'IDB via une connexion HTTPS (services Web). Il tourne sur le Gestionnaire de cellule et possède une connexion locale vers le service hpdp-idb-cp.

Configurer les variables d'environnement

Avant d'utiliser Data Protector, Micro Focus recommande que vous étendiez les valeurs spécifiques aux variables d'environnement de la configuration de votre système d'exploitation :

- Pour permettre de voir le manuel Data Protector de n'importe où, ajoutez /opt/omni/lib/man à la variable MANPATH.
- Pour permettre aux commandes de Data Protector d'être utilisées depuis n'importe quel répertoire, ajoutez les localisations des commandes à la variable PATH. Les procédures décrites dans la documentation de Data Protector considèrent que la valeur des variables a été étendue. Les localisations des commandes sont listées dans la page de référence omniintro que vous pouvez retrouver dans *Guide de référence de l'interface de ligne de commande Data Protector* et sur la page man relative à omniintro.

Étapes suivantes

À ce stade de l'installation, le Gestionnaire de cellule (et, le cas échéant, le Serveur d'installation) est installé pour les systèmes UNIX. Vos prochaines tâches sont :

1. Si vous n'avez pas installé de Serveur d'installation pour UNIX sur le même système, reportez-vous à Installing a UNIX Gestionnaire de cellule, Page 27.
2. Installez un Serveur d'installation pour Windows, si vous souhaitez installer à distance des logiciel pour clients Windows. Voir Installer un Serveur d'installation pour systèmes Windows, Page 45.
3. Distribuez le logiciel aux clients. Voir Installer des clients Data Protector, Page 54.

Installing a Windows Gestionnaire de cellule

Conditions préalables

- Une recherche DNS indirecte pour résoudre le nom d'hôte est requise pour tous les composants Data Protector de la cellule Data Protector.
- Le compte utilisateur utilisé pour l'installation doit :
  - Disposer des privilèges (`Administrator`) sur le système cible sélectionné.
  - Avoir accès aux droits utilisateurs configurés dans la stratégie de sécurité locale de Windows.
- Le service Data Protector Inet est exécuté par défaut par le compte utilisateur Windows local SYSTEM. Cependant, si pour diverses raisons le service Inet est lancé sous un compte utilisateur de domaine de Windows, vous devez lui accorder en plus les privilèges de Stratégie de sécurité suivants :
  - Emprunter l'identité d'un client après l'authentification
  - Remplacer un jeton de niveau processus

  Pour plus d'informations, reportez-vous à l'index *Aide de Data Protector*: "Emprunt d'identité d'utilisateur de service Inet".
- Le système qui deviendra le Gestionnaire de cellule doit :
  - Avoir un système d'exploitation Windows pris en charge installé. Pour avoir la liste des systèmes d'exploitation pris en charge pour le Gestionnaire de cellule, reportez-vous à https://softwaresupport.softwaregrp.com/.
  - Avoir suffisamment d'espace disque disponible pour le logiciel de Data Protector Gestionnaire de cellule. Le Gestionnaire de cellule nécessite un total de 4 GB de RAM.

    Pour la restauration de la base de données interne, le double de RAM totale est requis.

    Pour chaque session de sauvegarde parallèle, 40 MB de RAM sont requis. Par exemple, si vous voulez lancer 60 sessions de sauvegarde parallèles, 3 GB de RAM sont nécessaires.
  - Disposer d'un espace disque suffisant pour la base de données interne (IDB) Data Protector. 1,5 GB d'espace disque disponible et environ 100 bytes pour chaque fichier sauvegardé (pour être utilisé par l'IDB).

    Si vous ne disposez pas d'assez d'espace mémoire disponible sur le volume de disque sélectionné, vous pouvez monter un volume supplémentaire, mais vous devez le faire avant l'installation.

- Avoir `2 × size_of_the_biggest_package_to_be_installed + 10 MB` d'espace disque sur le lecteur système.
- Avoir un pare-feu configuré pour accepter les connexions «Administration des services à distance» (NP) (port 445).
- Disposer d'une implémentation Microsoft opérationnelle du protocole TCP/IP. Ce protocole doit pouvoir résoudre les noms d'hôte. Le nom de l'ordinateur et le nom de l'hôte doivent être identiques.
- Avoir une adresse IP statique assignée. Si le système est configuré en tant que client DHCP, son adresse IP change. C'est pourquoi il est demandé soit d'assigner une entrée DNS permanente au système (et de le reconfigurer), soit de configurer un serveur DHCP pour réserver une adresse IP statique pour le système (une adresse IP est liée à l'adresse MAC du système).
- Avoir les ports suivants disponibles :
  - 5565 — port requis pour une nouvelle installation dans Data Protector.
  - 5555 — port requis pour la mise à niveau de l'installation de Data Protector.
  - 7112 — port de service de la base de données interne
  - 7113 — port du pooler des connexions de la base de données interne (IDB CP)
  - 7116 — port du serveur d'application (HTTPS AS)
  - 9999 — port de gestion du serveur d'application

  Vous pouvez modifier les ports des services listés ci-dessus au cours de l'installation. Pour changer le numéro du port de communication par défaut, consultez le Changer le port Inet par défaut Data Protector, Page 354.

- Pour lancer un grand nombre de sessions sur un Gestionnaire de cellule Windows, il faut modifier la limite de taille de segment du bureau. La taille de chaque allocation de taille de segment de bureau est contrôlée par les valeurs de registre suivantes :

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

  La donnée par défaut pour cette valeur de registre ressemblera à :

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

  Les valeurs numériques suivant "SharedSection=" contrôlent la méthode d'allocation de la taille de segment du bureau. Ces valeurs SharedSection sont indiquées en kilobytes.
  - 1024 - taille de segment partagée, commune à tous les bureaux
  - 20480 - taille de segment de bureau pour chaque bureau associé à une station Windows interactive
  - 768 - taille de segment de bureau pour chaque bureau associé à une station Windows non interactive

Vous devez modifier la valeur de SharedSection associée à une station Windows non interactive pour la configurer sur 20480. Cette modification nécessite un redémarrage pour prendre effet.

Client Services de terminal Microsoft

- Pour installer Data Protector sur Windows avec le client Services de terminal Microsoft, assurez-vous Data Protectorque **Administration à distance** soit bien sélectionné pour le **Mode Terminal server** du système qui doit recevoir :
  1. Dans le Panneau de configuration Windows, cliquez sur **Outils d'administration**, puis sur **Configuration des services Terminal Server**.
  2. Dans la boîte de dialogue Configuration des services Terminal Server, cliquez sur **Paramètres du serveur**. Assurez-vous que le serveur Services de terminal soit bien lancé en mode Administration à distance.

Recommandations

- Si vous pensez que les fichiers binaires DC vont dépasser les 2 GB (leur taille n'est limitée que par les paramètres du système de fichiers), Micro Focus recommande l'utilisation du système de fichiers NTFS pour leur stockage.

Gestionnaire de cellule compatible cluster

Des conditions préalables et des étapes supplémentaires sont nécessaires pour l'installation d'un Gestionnaire de cellule compatible cluster. Voir Installation d'un Gestionnaire de cellule compatible cluster, Page 181.

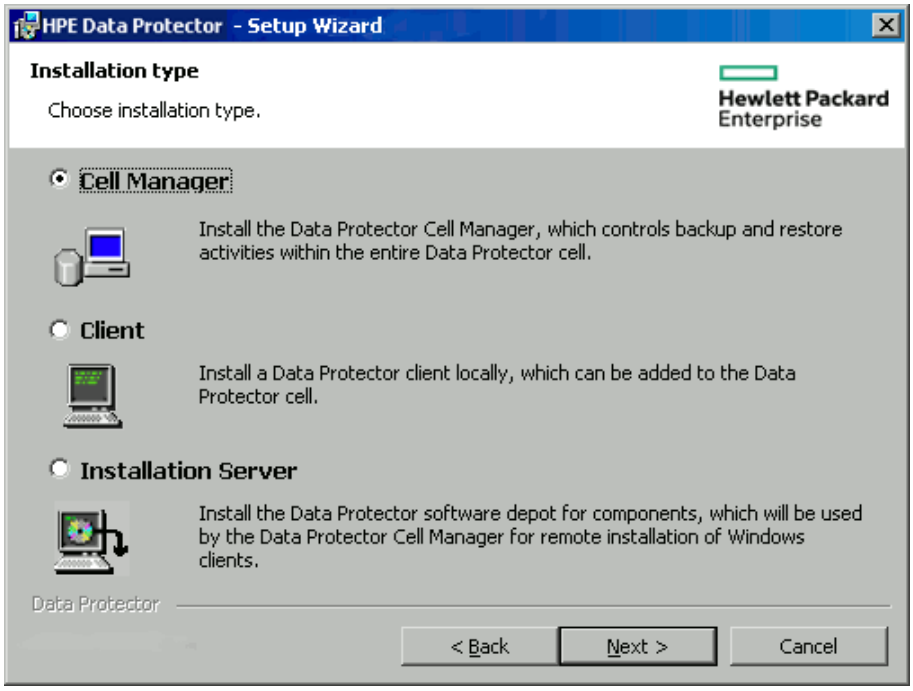
> **REMARQUE :**
> Dans un environnement à multiples cellules (MoM), tous les Gestionnaire de cellule doivent avoir la même version de Data Protector installée.

Procédure d'installation

Pour effectuer une nouvelle installation sur un système Windows

1. Copiez le package d'installation téléchargé (zip) sur le système Windows, et extrayez les fichiers vers un répertoire local. Exécutez le fichier `setup.exe` depuis le dossier applicable à votre plateforme.
2. Suivez les instructions de l'assistant et lisez attentivement le contrat de licence. Si vous en acceptez les conditions du contrat, cliquez sur **Suivant** pour continuer.
3. Examinez les détails dans la page Informations d'Obsolescence, et cliquez sur **Je comprends les modifications appliquées aux plateformes prises en charge**, uniquement si vous acceptez les modifications que Data Protector a appliquées à la liste des versions matérielles et logicielles prises en charge.
4. Sur la page Type d'installation, sélectionnez **Gestionnaire de cellule**, puis cliquez sur **Suivant** pour installer le logiciel Data ProtectorGestionnaire de cellule.

Sélectionner le type d'installation

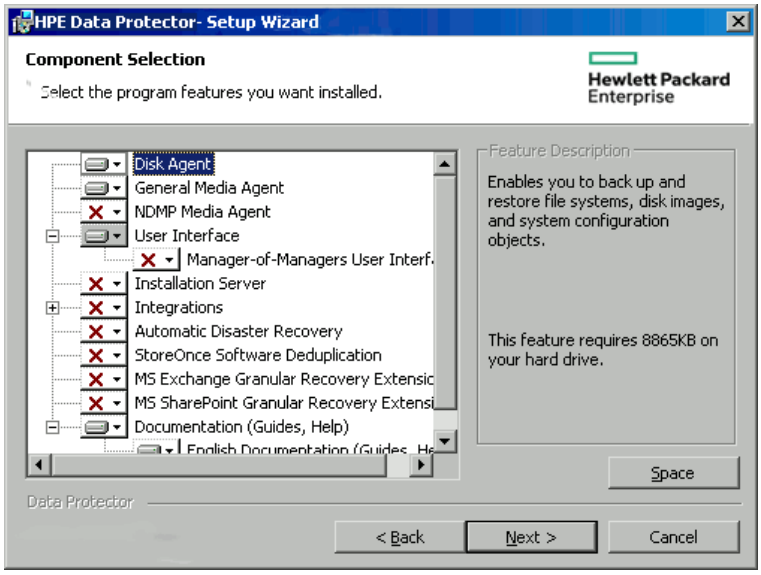


5. Indiquez le nom de l'utilisateur et le mot de passe du compte sur lequel les services Data Protector s'exécuteront.

   Cliquez sur **Suivant** pour continuer.
6. Cliquez sur **Suivant** pour installer Data Protector dans les dossiers d'installation par défaut.

   Sinon, cliquez sur **Changer** pour ouvrir la boîte de dialogue Changer le dossier de destination actuel ou Changer le dossier de destination des données du programme actuel, et changez le dossier d'installation comme requis. Le chemin vers le dossier d'installation des données du programme ne doit pas dépasser 80 caractères.
7. Sur la page Sélection des composants, sélectionnez les composants que vous souhaitez installer. Pour avoir une liste et une description des composants de Data Protector, reportez-vous à Composants Data Protector, Page 57.

Sélectionner les composants logiciels

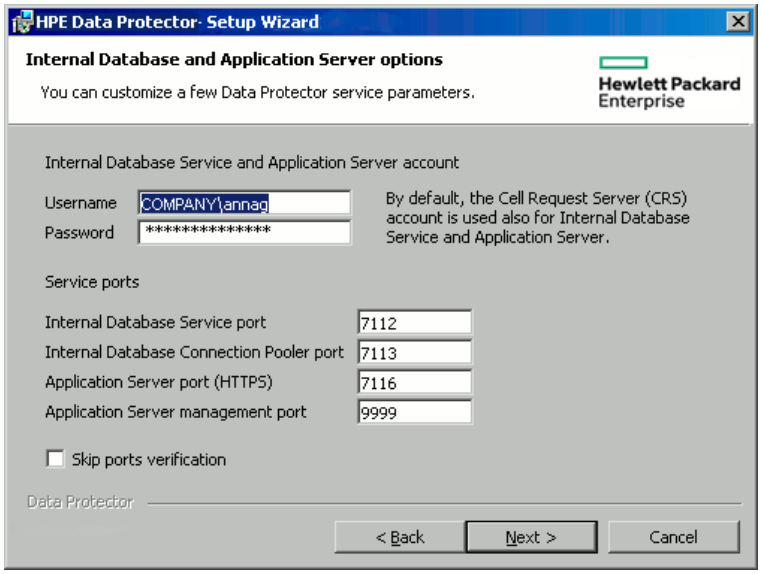


Agent de disque, **Agent de support général**, **Interface utilisateur**, et **Serveur d'installation** sont sélectionnés par défaut. Cliquez sur **Suivant**.

8. Vous pouvez, si vous le souhaitez, modifier le compte utilisateur utilisé par l'IDB et le Serveur d'application de Data Protector, ainsi que les ports utilisés par ces services.

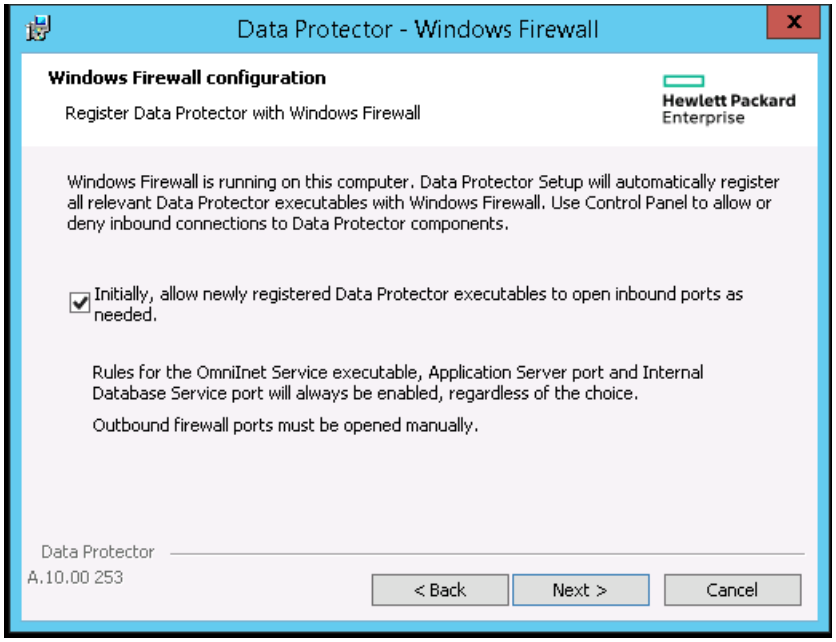
   Cliquez sur **Suivant**.

   Changer les options d'IDB et de Serveur d'application



9. Si Data Protector détecte Windows Firewall sur votre système, la page de configuration de Windows Firewall s'affiche. L'installation Data Protector détecte tous les exécutables Data Protector nécessaires. Par défaut, l'option **Permettre initialement aux nouveaux fichiers exécutables Data Protector enregistrés d'ouvrir des ports entrants le cas échéant** est sélectionnée. Si vous ne souhaitez pas permettre à Data Protector d'ouvrir les ports pour le moment, ne cochez pas l'option. Pour un fonctionnement correct de Data Protector avec

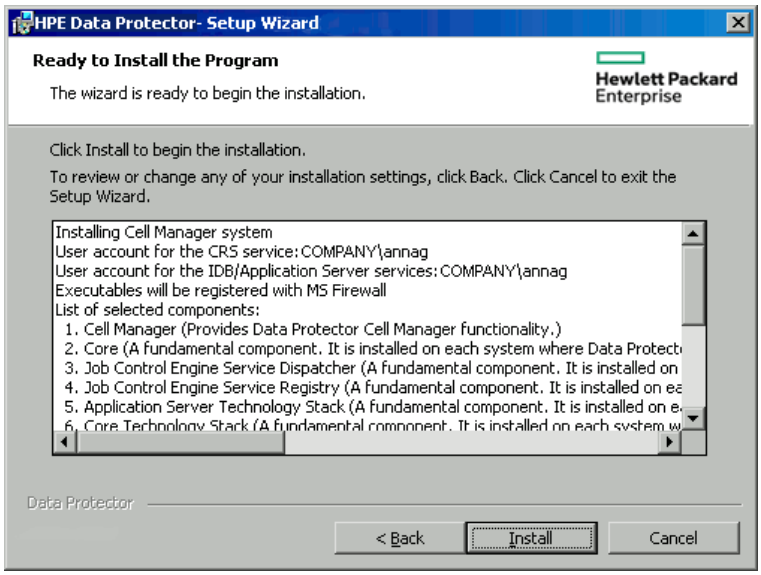
l'ancienne version des clients 10.00, les règles Data Protector doivent être activées dans le pare-feu Windows. Les règles pour l'exécutable Omnilnet Service, le port de Serveur d'application et le port de Service de base de données interne seront toujours activées, quel que soit votre choix.



Cliquez sur **Suivant**.

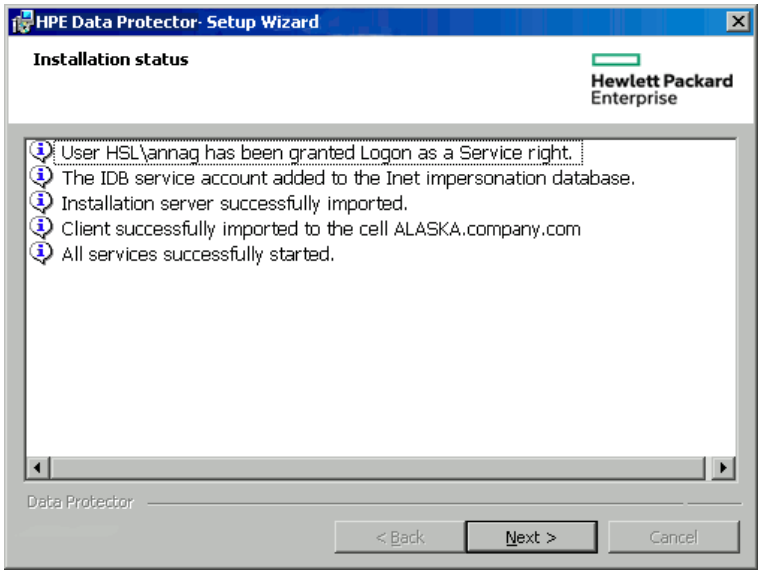
10. La liste des composants s'affiche. Cliquez sur **Installer** pour démarrer l'installation des composants sélectionnés. L'installation peut durer plusieurs minutes.

Résumé des composants



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

Page État de l'installation



12. Si vous avez installé le composant `User Interface`, pour commencer à utiliser l'interface utilisateur graphique Data Protector immédiatement après l'installation, sélectionnez **Lancer l'interface utilisateur graphique de Data Protector**.

    Si vous avez installé le composant `English Documentation (Guides, Help)`, pour voir les Annonces sur les produits, notes sur les logiciels et références Data Protector immédiatement après l'installation, sélectionnez **Références, notes de publication et annonces produits**.

    Cliquez sur **Terminer**.

Après l'installation

Les fichiers Gestionnaire de cellule sont situés dans le répertoire *répertoire_Data_Protector* et dans *données_programme_Data_Protector*.

Le dépôt de logiciel est situé dans le répertoire *données_programme_Data_Protector*`\Depot`.

Les localisations des commandes Data Protector sont situées dans les répertoires, listés dans la page de référence `omniintro` que vous pouvez retrouver dans *Guide de référence de l'interface de ligne de commande Data Protector* et dans le manuel `omniintro`.

> **IMPORTANT :**
> Micro Focus recommande que vous ajoutiez les localisations des commandes à la valeur de la variable d'environnement appropriée de votre système d'exploitation pour autoriser l'utilisation des commandes Data Protector depuis n'importe quel répertoire. Les procédures décrites dans la documentation de Data Protector considèrent que la valeur des variables a été étendue.

Les processus suivants sont lancés sur le système du Gestionnaire de cellule :

`crs.exe`	Le service Serveur de requête de la cellule (CRS) de Data Protector tourne sur le système du Gestionnaire de cellule et démarre quand le client du Gestionnaire de cellule est installé sur le système. Le CRS démarre et contrôle les sessions de sauvegarde et de restauration de la cellule. Il est exécuté dans le répertoire

	répertoire_Data_Protector\bin.
mmd.exe	Le service Démon de gestion des supports (MMD) de Data Protector est exécuté sur le système du Gestionnaire de cellule et démarre quand le client Gestionnaire de cellule est installé sur le système. Le MMD gère les opérations de gestion de périphérique et de support. Il est exécuté 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 Data Protector Inet doit être exécuté sur tous les systèmes dans la cellule Data Protector. Il est exécuté dans le répertoire *répertoire_Data_Protector*\bin.
kms.exe	Le service Serveur gestionnaire de clés (KMS) de Data Protector est exécuté sur le système du Gestionnaire de cellule et démarre quand le client Gestionnaire de cellule est installé sur le système. Ce service gère les clés pour la fonction de cryptage de Data Protector. Il est exécuté dans le répertoire *répertoire_Data_Protector*\bin.
hpdp-idb	Le service Data Protector Internal Database Service (hpdp-idb) est celui sous lequel s'exécute la base de données IDB. Le service est accédé localement sur le Gestionnaire de cellule par les processus qui ont besoin d'informations issues de la base de données interne. Ce service est accédé à distance uniquement pour les informations de gestion des supports sur le point d'être transférées de l'IDB du Gestionnaire de cellule vers l'IDB du Manager-of-Manager (MoM).
hpdp-idb-cp	Le service Data Protector Internal Database Connection Pooler (hpdp-idb-cp) propose un pool de connexions ouvertes à hpdb-idb qui peuvent être utilisées à la demande au lieu d'ouvrir une nouvelle connexion pour chaque requête, ce qui permet d'assurer l'extensibilité de la connexion hpdb-idb. Le service tourne sur le Gestionnaire de cellule et ne peut être accédé que par des processus locaux.
hpdp-as	Le service Data Protector Application Server (hpdp-as) est utilisé pour la connexion de l'interface graphique à l'IDB via une connexion HTTPS (services Web). Il tourne sur le Gestionnaire de cellule et possède une connexion locale vers le service hpdp-idb-cp.

REMARQUE :
Si vous envisagez d'utiliser l'interface utilisateur de Data Protector pour effectuer des sauvegardes ou des restaurations entre plateformes, consultez Annonces sur les produits, notes sur les logiciels et références Data Protector pour connaître les limitations que cela engendre.

CONSEIL :
Vous pouvez installer des tables de conversion des pages de codes pour afficher correctement les noms de fichiers, si le codage correspondant n'est pas disponible dans l'interface graphique de Data Protector. Pour connaitre les instructions détaillées, consultez la documentation de votre système d'exploitation.

Dépannage

En cas d'échec de l'installation, consultez les conditions préalables vérifiées par `Setup` elle-même et qui pourraient causer l'échec si elles n'ont pas été remplies. Voir Conditions préalables, Page 34.

Voici une liste des conditions préalables vérifiées par `Setup` :

- Version du Service Pack
- `nslookup`, pour que Data Protector soit en mesure de développer les noms d'hôte
- espace disque
- droits d'administration

Étapes suivantes

À ce stade de l'installation, le Gestionnaire de cellule (et, le cas échéant, le Serveur d'installation) est installé pour les systèmes Windows. Vos prochaines tâches sont :

1. Installer le Serveur d'installation pour UNIX, si vous avez un environnement de sauvegarde mixe. Voir Installation du Gestionnaire de cellule et des Serveur d'installationde Data Protector, Page 26. Sautez cette étape si vous n'avez pas besoin du Serveur d'installation pour système UNIX.
2. Distribuez le logiciel aux clients. Voir Installer des clients Data Protector, Page 54.

Installation de Serveur d'installation

Des Serveur d'installation peuvent être installés sur le système du Gestionnaire de cellule ou sur n'importe quel système pris en charge connecté en LAN au Gestionnaire de cellule. Pour en savoir plus sur les systèmes d'exploitation pris en charge pour le Serveur d'installation, reportez-vous à https://softwaresupport.softwaregrp.com/.

Pour garder les Serveur d'installations sur des systèmes séparés du Gestionnaire de cellule, installez localement les dépôts de logiciel correspondants. La procédure détaillée est décrite dans cette section.

Installer des Serveur d'installation pour systèmes UNIX

Conditions préalables

Le système qui deviendra votre Serveur d'installation doit remplir les conditions préalables suivantes :

- Avoir un système d'exploitation HP-UX ou Linux installé. Pour plus de détails sur les systèmes d'exploitation pris en charge pour le Serveur d'installation, consultez le Annonces sur les produits, notes sur les logiciels et références Data Protector.
- Inclure le démon `inetd` ou `xinetd` opérationnel.
- Une recherche DNS indirecte pour résoudre le nom d'hôte est requise pour tous les composants

Data Protector de la cellule Data Protector.

- Avoir le numéro de port 5555/5565 (par défaut) disponible. Si tel n'est pas le cas, voir Changer le port Inet par défaut Data Protector, Page 354.
- Disposer du protocole TCP/IP installé et en exécution. Ce protocole doit pouvoir résoudre les noms d'hôte.
- Disposer de suffisamment d'espace disque pour l'intégralité du dépôt de logiciel de Data Protector. Les spécifications minimales suivantes sont requises :
  - Un total de 512 Mo de RAM
  - 1,5 Go d'espace disque disponible
- Vous devez disposer soit d'un accès `root`, soit d'un compte avec des privilèges root.
- Le Gestionnaire de cellule dans la cellule Data Protector doit être de la version10.00 .

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

`/opt/omni/ -> /prefix/opt/omni/`

`/etc/opt/omni/ -> /prefix/etc/opt/omni/`

`/var/opt/omni/ -> /prefix/var/opt/omni/`

Créez les liens avant l'installation et assurez-vous que le répertoire de destination existe.

REMARQUE :
Pour installer un logiciel depuis un périphérique situé sur le réseau, vous devez avant tout monter le dossier source sur votre ordinateur.

Recommandations

Utiliser un Data Protector UNIX pour installer Serveur d'installation est la méthode recommandée pour les clients UNIX.

L'installation locale de Data Protector sur des clients UNIX est possible mais n'est pas recommandée : il n'existe pas de procédure prise en charge pour mettre à jour des clients UNIX sans Serveur d'installation.

Étant donné qu'un Serveur d'installation est requis pour mettre à jour les clients UNIX, Il est recommandé d'utiliser ce même Serveur d'installation pour installer Data Protector sur les clients UNIX.

Procédure d'installation

Pour installer le Serveur d'installation pour système UNIX sur un système HP-UX ou Linux

1. Copiez le package d'installation Data Protector téléchargé (tar) sur le système HP-UX ou Linux et extrayez les fichiers vers un répertoire local.

   `LOCAL_INSTALL`

platform_dir/DP_DEPOT

Où *rép_plateforme* est :

hpux	pour les systèmes HP-UX
linux_x86_64	pour les systèmes Linux

2. Allez dans le répertoire LOCAL_INSTALL et exécutez :

   ```
   ./omnisetup.sh -IS
   ```

   Pour obtenir une description de la commande omnisetup.sh, reportez-vous au fichier README situé dans le package d'installation (tar), *Mount_point/* ou *Guide de référence de l'interface de ligne de commande Data Protector* situé dans le répertoire DOCS/C/MAN du package d'installation.

Lorsque l'installation est terminée, le dépôt du logiciel pour UNIX se trouve dans le répertoire /opt/omni/databases/vendor.

La commande omnisetup.sh installe le Serveur d'installationavec tous les packages. Pour n'installer qu'une partie des packages, utilisez swinstall(pour HP-UX) ou rpm(pour Linux). Voir Installer sur des systèmes HP-UX et Linux avec des outils natifs, Page 343.

> **IMPORTANT :**
> Si vous n'installez pas de Serveur d'installation pour UNIX sur votre réseau, il vous faudra installer localement chaque client UNIX à partir du package d'installation UNIX (tar) (pour HP-UX ou Linux). Qui plus est, il sera impossible de mettre à jour les composants des clients Data Protector.

Étapes suivantes

À ce stade là, les Serveur d'installation pour UNIX devraient être installés sur votre réseau. Vos prochaines tâches sont :

1. Si vous avez installé le Serveur d'installation sur un système différent du Gestionnaire de cellule, vous devez ajouter (importer) manuellement le système à la celluleData Protector . Voir Installer des Serveur d'installation pour systèmes UNIX, Page 42.

   > **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 pour lister les packages d'installation distante qui ont été installés. Vous pouvez vérifier les packages d'installation distantes disponibles depuis l'interface en ligne de commande. Pour assurer que ce fichier reste à jour, il est recommandé d'exporter et de réimporter un Serveur d'installation à chaque fois que des packages d'installation distante sont installés ou supprimés. Cela s'applique même si un Serveur d'installation est installé sur le même système que le Gestionnaire de cellule.

2. Si des systèmes sous Windows sont présents dans votre cellule Data Protector, installez le Serveur d'installation pour Windows. Voir Installer un Serveur d'installation pour systèmes Windows, Page suivante.
3. Distribuez le logiciel aux clients. Voir Installer des clients Data Protector, Page 54.

Installer un Serveur d'installation pour systèmes Windows

Conditions préalables

Le système qui deviendra votre Serveur d'installation doit posséder les spécifications suivantes :

- Un système d'exploitation Windows pris en charge. Pour en savoir plus sur les systèmes d'exploitation pris en charge pour le Serveur d'installation, reportez-vous à https://softwaresupport.softwaregrp.com/.
- Disposer de suffisamment d'espace disque pour l'intégralité du dépôt de logiciel de Data Protector. Les spécifications minimales suivantes sont requises :
  - Un total de 512 MB de RAM
  - 2 GB d'espace disque disponible
- Une recherche DNS indirecte pour résoudre le nom d'hôte est requise pour tous les composants Data Protector de la cellule Data Protector.
- TCP/UDP 445. Pour l'installation par chargement du nouveau client Data Protector (sans composants Data Protectorsur le client), un partage de serveur d'installation accessible est requis. Une autre possibilité est que, si le partage de dépôt Serveur d'installation n'est pas accessible, l'installation initiale du client Data Protector doit s'effectuer localement.
- 5565 : port nécessaire pour la nouvelle installation dans Data Protector. Si tel n'est pas le cas, voir Changer le port Inet par défaut Data Protector, Page 354.
- 5555 : port nécessaire lors de la mise à niveau de l'installation Data Protector.
- Implémentation Microsoft du protocole TCP/IP opérationnelle. Ce protocole doit pouvoir résoudre les noms d'hôte. Le nom de l'ordinateur et le nom de l'hôte doivent être identiques.

Limites

Compte tenu des restrictions de sécurité imposées par le système d'exploitation Windows, l'une des conditions suivantes doit être vérifiée :

- Ni le serveur d'installation, ni le client ne se trouvent dans le même domaine.
- Le serveur d'installation et le client se trouvent dans le même domaine.

IMPORTANT :
Si vous n'installez pas le Serveur d'installation pour Windows sur votre réseau, vous devrez installer localement chaque client Windows à partir du package d'installation (zip).

REMARQUE :
Vous ne pouvez installer à distance un client Data Protector sur un système Windows si un Serveur d'installation a déjà été installé sur le système. Pour installer un Serveur d'installation et un ou des composants client sur le même système, vous devez lancer l'installation du client

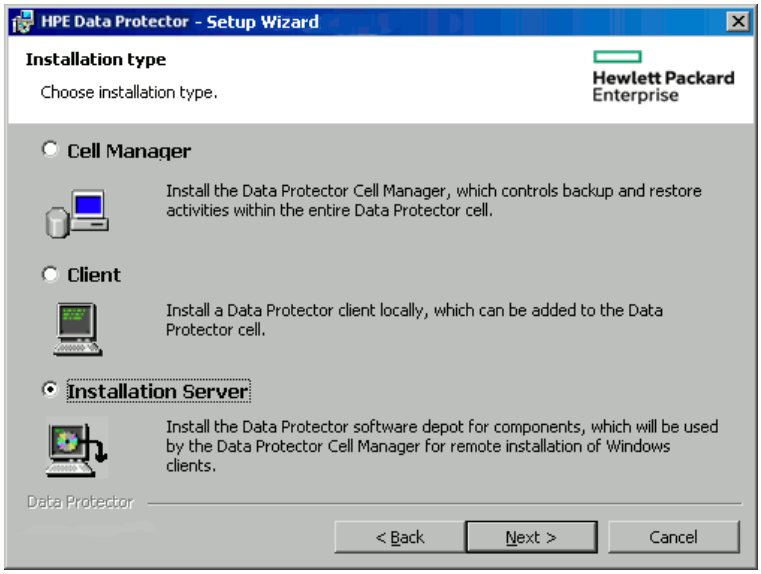
> en local. Pendant la procédure d'installation, sélectionnez tous les composants client désirés et le composant Serveur d'installation. Voir Installer des clients Data Protector, Page 54.

Procédure d'installation

Pour installer le Serveur d'installation sur un système Windows

1. Copiez le package d'installation téléchargé (zip) sur un système Windows et décompressez les fichiers dans un répertoire local. Exécute le fichier `setup.exe` à partir du dossier correspondant à votre plate-forme.
2. Suivez les instructions de l'assistant et lisez attentivement le contrat de licence. Si vous en acceptez les conditions du contrat, cliquez sur **Suivant** pour continuer.
3. Examinez les détails de la page Informations d'obsolescence et cliquez sur **Je comprends les changements apportés aux plates-formes prises en charges**, uniquement si vous acceptez modifications apportées par Data Protector à la liste des versions logicielles et matérielles prises en charge.
4. Dans la page **Type d'installation**, sélectionnez Serveur d'installation puis cliquez sur **Suivant** pour installer le dépôt de logiciel de Data Protector.

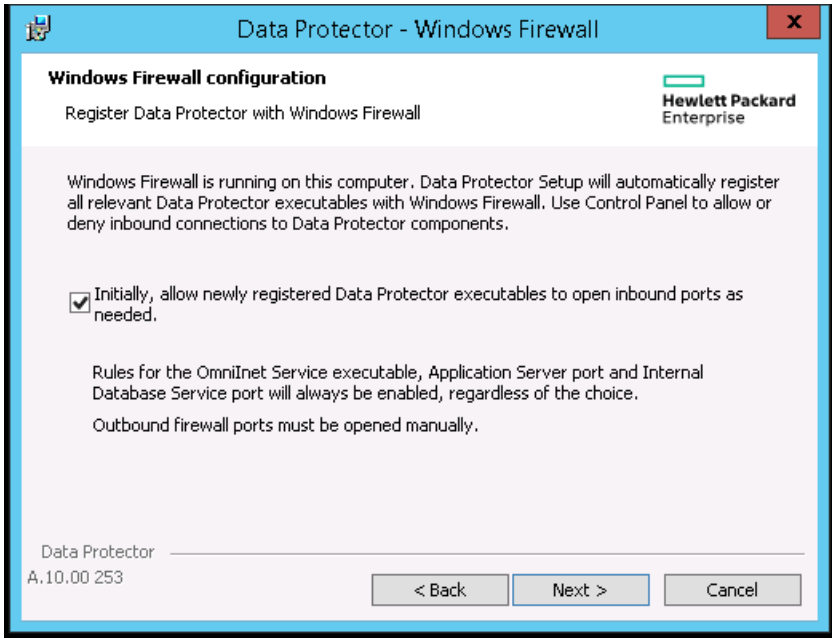
   Sélectionner le type d'installation

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

   Sinon, cliquez sur **Modifier** pour ouvrir la fenêtre Modifier le dossier de destination actuel et entrez un autre chemin.
6. Si Data Protector détecte Windows Firewall sur votre système, la page de configuration de Windows Firewall s'affiche. Le processus de configuration de Data Protector enregistre tous les exécutables Data Protector. 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 permettre à Data Protector d'ouvrir les ports pour le moment, ne cochez pas l'option. Pour un fonctionnement correct de Data Protector avec la version précédente des clients 10.00, les règles Data Protector dans le pare-feu Windows doivent être activées. Les

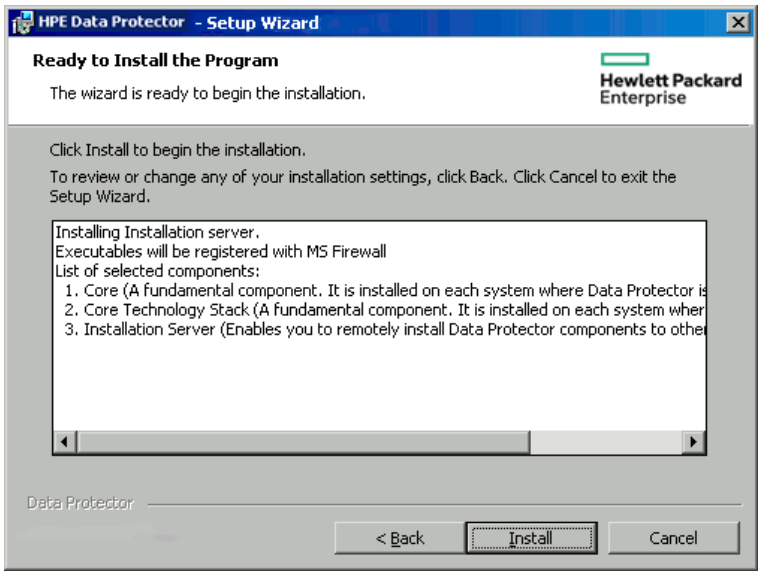
règles pour l'exécutable du service OmniInet, le port du serveur d'application et le port de l'IDS seront toujours activées, indépendamment du choix effectué.



Cliquez sur **Suivant**.

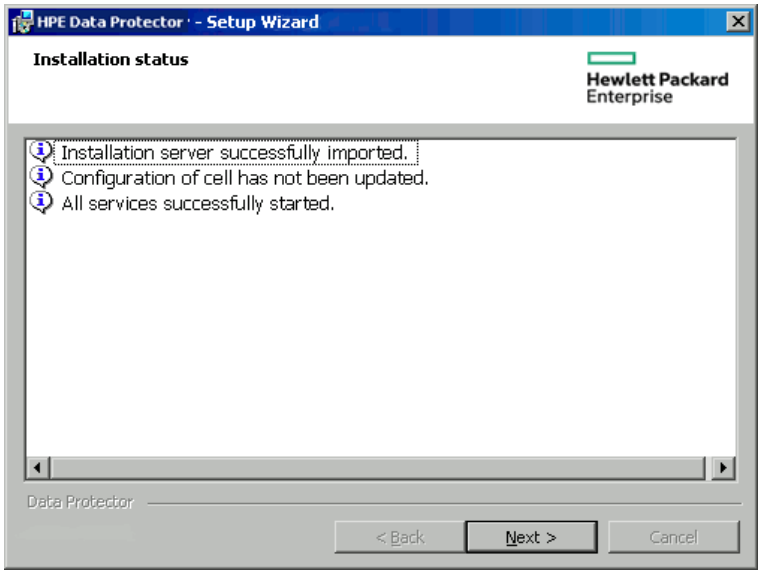
7. La liste des composants s'affiche. Cliquez sur **Installer** pour démarrer l'installation des composants sélectionnés. L'installation peut durer plusieurs minutes.

   Écran de résumé de la sélection des composants



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

Page État de l'installation



9. Cliquez sur **Terminer**.

Une fois l'installation terminée, le logiciel est, par défaut, installé dans le répertoire *données_programme_Data_Protector*\Depot. Le logiciel est partagé afin d'être accessible depuis le réseau.

Afin que les fichiers d'installation ne soient pas changés pendant la copie du serveur d'installation vers un nouveau client, le protocole de fichier de serveur SMB (Session Management Block) est utilisé pour la communication entre Serveur d'installation et le client.

Le serveur d'installation configure la signature du paquet SMB pendant la première installation à distance. Les stratégies suivantes sont appliquées :

- Client réseau Microsoft : Signature numérique des communications (toujours)
- Serveur réseau Microsoft : Signature numérique des communications (toujours)

Les valeurs de registre suivantes du paramètre **RequireSecuritySignature** seront définies sur 1 au niveau des clés suivantes :

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

Le message suivant s'affiche pendant l'installation à distance :

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

Après l'activation de la signature SMB, si un utilisateur souhaite se connecter à un autre hôte à partir de l'hôte du serveur d'installation via SMB, la signature SMB doit également être activée sur cet autre hôte.

Étapes suivantes

À ce stade-là, les Serveur d'installation pour Windows devraient être installés sur votre réseau. Il est à présent recommandé d'effectuer les tâches suivantes :

1. Si vous avez mis en place un Serveur d'installation indépendant (c'est à dire, qui n'est pas sur le Gestionnaire de cellule), vous devez ajouter (importer) manuellement le système à la cellule de Data Protector.
   Voir Installer des Serveur d'installation pour systèmes UNIX, Page 42.
2. Installez un Serveur d'installation pour UNIX sur HP-UX ou Linux si votre environnement de sauvegarde est mixte. Voir Installer des Serveur d'installation pour systèmes UNIX, Page 42.
3. Distribuez le logiciel aux clients. Voir Installer des clients Data Protector, Page 54.

Installation de Data Protector Single Server Edition

La Single Server Edition (SSE) de Data Protector a été créée pour les environnements de petite taille où les sauvegardes ne sont exécutées sur que un périphérique connecté à un Gestionnaire de cellule. Elle est disponible pour les plateformes Windows et HP-UX prises en charge.

Pour installer le Gestionnaire de cellule et (en option) Serveur d'installation, suivez les instructions Installation du Gestionnaire de cellule et des Serveur d'installationde Data Protector, Page 26.

Restrictions de SSE pour Windows

- SSE prend en charge les sauvegardes pour un seul périphérique à la fois connecté à un seul Gestionnaire de cellule.
- Un seul changeur automatique 10-slot DDS est pris en charge.
- Les clients et serveurs UNIX (et HP-UX) ne sont pas pris en charge. Si une sauvegarde est tentée sur une machine UNIX, la session est annulée.
- L'ajout de produits d'extension n'est pas pris en charge avec SSE.
- La gestion des clusters n'est pas prise en charge avec SSE.
- La récupération après sinistre n'est pas prise en charge avec SSE.

Le nombre de clients Windows n'est pas limité.

Pour connaître les périphériques pris en charge, reportez-vous à la section Annonces sur les produits, notes sur les logiciels et références Data Protector.

Restrictions de SSE pour HP-UX

- SSE prend en charge les sauvegardes pour un seul périphérique à la fois connecté à un seul Gestionnaire de cellule.
- Un seul changeur automatique 10-slot DDS est pris en charge.
- Sur un Gestionnaire de cellule UNIX, vous ne pouvez pas sauvegarder de serveurs - uniquement des clients UNIX, Windows et Solaris.
- L'ajout de produits d'extension n'est pas pris en charge avec SSE.
- La gestion des clusters n'est pas prise en charge avec SSE.

Le nombre de clients (UNIX, Windows) n'est pas limité.

Pour connaître les périphériques pris en charge, reportez-vous à la section Annonces sur les produits, notes sur les logiciels et références Data Protector.

Mettre en place un mot de passe

Pour connaitre les instructions étape par étape pour mettre un mot de passe sur le Gestionnaire de cellule, reportez-vous à Mots de passe Data Protector, Page 309.

Vérification de l'installation

Pour contrôler si les composants logiciels Data Protector sont en cours d'exécution sur le Gestionnaire de cellule ou sur les systèmes client, vous pouvez vérifier l'installation à l'aide de l'interface utilisateur graphique Data Protector.

Conditions préalables

Vous devez disposer du serveur d'installation correspondant au type de système client (système UNIX ou système Windows) que vous utilisez.

Procédure

1. Dans la liste de contexte, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, développez l'élément **Clients**, cliquez avec le bouton droit de la souris sur le Gestionnaire de cellule ou le système client, puis cliquez sur **Vérifier installation** pour ouvrir l'assistant.
3. La liste de tous les systèmes client du même type (systèmes UNIX ou systèmes Windows) s'affiche. Sélectionnez les clients dont vous souhaitez vérifier l'installation, puis cliquez sur **Terminer** pour démarrer la vérification.

Les résultats de la vérification s'affichent dans la fenêtre Vérifier installation.

À propos de la configuration du service Inet Data Protector

Sur les systèmes Windows, les sessions de sauvegarde et de restauration sont lancées par le service Inet Data Protector qui, par défaut, s'exécute sous le compte utilisateur local Windows SYSTEM. Par conséquent, les sessions de sauvegarde et de restauration se déroulent sous le même compte utilisateur.

Intégrations

Certaines intégrations de Data Protector nécessitent que les sessions de sauvegarde et de restauration soient lancées sous un compte utilisateur de domaine Windows. Sur le système Windows Server 2003, il suffit pour satisfaire cette exigence de relancer le service Inlet Data Protector sous un

compte utilisateur différent. Cela n'est plus possible pour les autres systèmes d'exploitation Windows pris en charge. Ainsi, Data Protector fait appel à un autre concept : emprunt d'identité d'utilisateur . Cette fonction permet au service Inet Data Protector, même s'il s'exécute sous le compte utilisateur local Windows SYSTEM, d'emprunter l'identité d'un compte utilisateur de domaine Windows et de démarrer l'agent d'intégration sous ce compte.

Pour activer l'emprunt d'identité d'utilisateur du service Inet Data Protector, vous devez indiquer le compte utilisateur de domaine Windows dans la spécification de sauvegarde ou dans l'assistant de restauration. Le compte utilisateur et le mot de passe associé doivent en outre être enregistrés dans la base de registre Windows.

Exécuter le service Inet sous un compte utilisateur de domaine Windows

Dans certains cas, le service Inet Data Protector doit s'exécuter sous un compte utilisateur de domaine Windows :

- **Environnements de cluster**

  Dans un cluster, vous devez configurer le service Inet Data Protector pour tous les nœuds de cluster. Cela signifie que vous devez utiliser un compte utilisateur de domaine Windows comme compte Inet.

Lorsque le service Inet s'exécute sous un compte utilisateur de domaine Windows, vous devez lui accorder les privilèges de stratégie de sécurité du système d'exploitation Windows suivants :

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

Configuration d'un compte utilisateur pour l'emprunt d'identité d'utilisateur du service Inet Data Protector

Vous pouvez faire en sorte que le service Inet Data Protector, qui s'exécute par défaut sous le compte utilisateur local Windows SYSTEM, utilise un autre compte utilisateur de domaine Windows pour démarrer une session.

- Configurez le compte utilisateur comme suit :
  - Accordez à l'utilisateur l'autorisation d'accès aux données (données applicatives, par exemple).
  - Assurez-vous que l'utilisateur a été ajouté au groupe d'utilisateurs Data Protector`admin` ou opérateur de `operator`.

Utilisation de l'interface graphique de Data Protector

Procédure

1. Dans la liste de contexte, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, développez **Data Protector Cellule**, puis **Clients**.
3. Cliquez avec le bouton droit de la souris sur le client, puis sélectionnez **Ajouter emprunt d'identité**.

   > **REMARQUE :**
   > Pour modifier ou supprimer un utilisateur, cliquez sur **Modifier emprunt d'identité** ou **Supprimer emprunt d'identité**.

4. Dans la page Sélectionner systèmes client, sélectionnez les systèmes clients pour lesquels vous voulez configurer l'emprunt d'identité d'utilisateur du service Inet Data Protector, puis cliquez sur **Suivant**.
5. Dans la page d'ajout, de suppression ou de modification d'emprunt d'identité, ajoutez un nouveau compte utilisateur ou modifiez ou supprimez un compte existant, puis cliquez sur **Terminer**.

> **IMPORTANT :**
> Le compte utilisateur enregistré dans la base de registre Windows sera utilisé par le service Inet Data Protector au moment voulu.

Utilisation de l'interface de ligne de commande Data Protector

- Pour configurer un compte utilisateur pour l'emprunt d'identité d'un client Data Protector, utilisez la commande `omniinetpasswd`.

  Ouvrez une session sur le client et exécutez la commande suivante :

  ```
  omniinetpasswd –add User@DomainPassword
  ```

- Pour configurer un compte utilisateur pour l'emprunt d'identité de plusieurs clients Data Protector, utilisez la commande `omnicc`.

  Ouvrez une session sur le Gestionnaire de cellule et exécutez la commande suivante :

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

Pour plus d'informations sur les commandes `omniinetpasswd` et `omnicc` , reportez-vous au document *Guide de référence de l'interface de ligne de commande Data Protector*.

Modifier le compte Inet Data Protector

Pour garantir que le service Inet Data Protector démarre les processus nécessaires pour la sauvegarde et la restauration sous un compte utilisateur spécifique, vous devez redémarrer le service sous ce

compte utilisateur.

Conditions préalables

- Microsoft Cluster Server : Avant de modifier le compte, placez les groupes de clusters OBVS_HPDP_AS, OBVS_HPDP_IDB, OBVS_HPDP_IDB_CP et OBVS_MCRS hors ligne. Une fois que le service Inet Data Protector a redémarré sous un compte différent, remettez les groupes de clusters en ligne.

Sur les systèmes Windows

1. Dans le Panneau de configuration, cliquez sur Outils d'administration, puis sur Services.
2. Cliquez deux fois sur **Inet Data Protector.**
3. Dans la boîte de propriétés générales d'Inet Data Protector, cliquez sur **Arrêt,** puis sur l'onglet **Connexion**.
4. Cliquez sur **le bouton C**e compte.
5. Saisissez le nom du compte possédant l'autorisation appropriée (pour accéder au disque partagé) ou sélectionnez-le.
6. Saisissez, puis confirmez le mot de passe.
7. Cliquez sur OK pour quitter ces pages de propriétés.
8. Assurez-vous que Inet Data Protector soit toujours sélectionné, cliquez dessus avec le bouton droit, puis cliquez sur **Démarrer**.
9. Quittez cette boîte de dialogue.

Chapitre 3: Installer des clients Data Protector

Vous pouvez installer des clients Data Protectorà distance, en les distribuant grâce au Serveur d'installation, ou localement, depuis le package d'installation (zip/tar) approprié.

Utiliser un Data Protector UNIX pour installer Serveur d'installation est la méthode recommandée pour les clients UNIX.

L'installation locale de Data Protector sur des clients UNIX est possible mais n'est pas recommandée : il n'existe pas de procédure prise en charge pour mettre à jour des clients UNIX sans Serveur d'installation.

Étant donné qu'un Serveur d'installation est requis pour mettre à jour les clients UNIX, Il est recommandé d'utiliser ce même Serveur d'installation pour installer Data Protector sur les clients UNIX.

> **REMARQUE :** Un Serveur d'installation Windows cible le port 445 d'un client lors d'une installation à distance, alors qu'un Serveur d'installation HP-UX/Linux cible le port 22 d'un client (installation à distance sécurisée) ou les ports 512 / 514 (installation à distance non sécurisée). Du côté Serveur d'installation, des ports éphémères sont utilisés pour établir les connexions à ces ports cibles.

Une fois les clients installés, Micro Focus vous recommande d'activer les appels de commandes Data Protector depuis n'importe quel répertoire en ajoutant les localisations des commandes à la variable d'environnement correspondante sur chaque client. Les procédures décrites dans la documentation de Data Protector considèrent que la valeur des variables a été étendue. Les localisations des commandes sont listées dans la page de référence `omniintro` que vous pouvez retrouver dans *Guide de référence de l'interface de ligne de commande Data Protector* et sur la page man relative à `omniintro`.

Une fois les clients Data Protector installés et importés dans la cellule, il est grandement recommandé de vérifier l'installation et de protéger les clients d'accès injustifiés. Pour connaitre la procédure de vérification de l'installation du client, consultez Vérification de l'installation client de Data Protector, Page 332. Pour plus d'informations sur la protection de sécurité, consultez À propos de la sécurité, Page 200.

Installer des systèmes clients Data Protector

Système client	Type d'installation et référence
Windows	Installation locale et à distance, voir Installation de clients Windows, Page 62
HP-UX	Installation locale et à distance, voir Installation de clients HP-UX , Page 71
Solaris	Installation locale et à distance, voir Installation de clients Solaris, Page 75
Linux	Installation locale et à distance, voir Installation de clients Linux, Page 82
Serveur ESX	Installation locale et à distance, voir Installation de clients ESX Server, Page 85
Mac OS X	Installation locale et à distance, voir Installer des clients Mac OS X, Page 87

Système client	Type d'installation et référence
IBM AIX	Installation locale et à distance, voir Installation de clients IBM AIX, Page 85
HP OpenVMS	Installation locale; voir Installation de clients OpenVMS HP, Page 89
Autres systèmes UNIX	Installation locale; voir Installation locale sur les systèmes UNIX et Mac OS X, Page 103
Client Agent de support DAS	Installation à distance et en local; consultez Installation d'un Agent de support pour utiliser la bibliothèque ADIC/GRAU ou la StorageTek Library, Page 106.
Client Agent de support ACS	Installation locale et à distance, voir Installation d'un Agent de support pour utiliser la bibliothèque ADIC/GRAU ou la StorageTek Library, Page 106

Intégrations

Les intégrations Data Protector sont des composants logiciel qui vous permettent de sauvegarder les applications de base de données avec Data Protector. Les systèmes qui exécutent les applications de base de données sont installés comme n'importe quel système client Windows ou UNIX, pour peu que le composant logiciel approprié ait bien été sélectionné (par exemple, le composant `MS Exchange Integration` pour sauvegarder une base de données de Microsoft Exchange Server, ou le composant `Oracle Integration` pour sauvegarder une base de données Oracle, et ainsi de suite).

Installer des intégrations

Application logicielle ou famille de baies de disques	Référence
Microsoft Exchange Server	Voir Clients Microsoft Exchange Server, Page 116.
Microsoft SQL Server	Voir Clients Microsoft SQL Server, Page 123
Serveur Microsoft SharePoint	Voir Clients Microsoft SharePoint Server, Page 123
Microsoft Volume Shadow Copy Service (VSS)	Voir Clients de Microsoft Volume Shadow Copy Service, Page 127.
Serveur Sybase	Voir Clients Sybase Server, Page 128
Serveur Informix	Voir Clients Informix Server, Page 128

Application logicielle ou famille de baies de disques	Référence
SAP R/3	Voir Clients SAP R/3, Page 129
SAP MaxDB	Voir Clients SAP MaxDB, Page 129
Appareil SAP HANA	Voir Clients SAP HANA Appliance, Page 129
Serveur Oracle	Voir Clients Oracle Server, Page 130
MySQL	Voir Clients MySQL, Page 130
PostgreSQL	Voir Clients PostgreSQL, Page 131
IBM DB2 UDB	Voir Clients IBM DB2 UDB, Page 131
Serveur Lotus Notes/Domino	Voir Clients Lotus Notes/Domino Server, Page 131
VMware	Voir Clients VMware, Page 132
Microsoft Hyper-V	Voir Clients Microsoft Hyper-V, Page 140
Serveur NDMP (Network Data Management Protocol)	Voir Clients NDMP Server, Page 141
Solutions P4000 SAN	Voir Solutions P4000 SAN clients, Page 142
Famille de baies de disques P6000 EVA	Voir Famille de baies de disques P6000 EVA clients, Page 142
Famille de baies de disque P9000 XP	Voir Famille de baies de disque P9000 XP clients, Page 148
Stockage 3PAR StoreServ	Voir 3PAR StoreServ Storage clients, Page 154
EMC Symmetrix	Voir Clients EMC Symmetrix, Page 154
Fournisseur de stockage EMC VNX	Voir Baies de stockage non HPE, Page 159
Fournisseur de	Voir Baies de stockage non HPE, Page 159

Application logicielle ou famille de baies de disques	Référence
stockage EMC VMAX	
Fournisseur de stockage NetApp	Voir Baies de stockage non HPE, Page 159

Autres installations

Installation	Référence
Serviceguard	Voir Installation de Data Protector sur Serviceguard, Page 166.
Symantec Veritas Cluster Server	Voir Installation de Data Protector sur Symantec Veritas Cluster Server, Page 177.
Serveur de Cluster Microsoft	Voir Installation de Data Protector sur Microsoft Cluster Server, Page 180.
IBM HACMP Cluster	Voir Installation de Data Protector sur un cluster IBM HACMP, Page 192.
Grappe Microsoft Hyper-V	Voir Installation de Data Protector sur un cluster Microsoft Hyper-V, Page 192.

Composants Data Protector

Pour connaître les dernières informations au sujet des plates-formes prises en charge, visitez la page d'accueil de Data Protector à l'adresse suivante : https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.

Voici les composants Data Protector que vous pouvez sélectionner ainsi que leur description :

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

	REMARQUE : Les commandes spécifiques de l'interface en ligne de commande de Data Protector sont inclues avec les autres composants Data Protector. Pour plus de détails, reportez-vous à *Guide de référence de l'interface de ligne de commande Data Protector*. Avant d'utiliser l'interface utilisateur Data Protector dans des environnements hétérogènes, consultez Annonces sur les produits, notes sur les logiciels et références Data Protector pour connaître les restrictions applicables.
Documentation en français (Guides, Aide)	Fichiers de documentations de Data Protector en anglais.
Composant Documentation française (Guides, Aide).	Fichiers de documentations de Data Protector en français.
Composant Documentation japonaise (Guides, Aide).	Fichiers de documentations de Data Protector en japonais.
Composant Documentation chinoise simplifiée (Guides, Aide).	Fichiers de documentations de Data Protector en chinois simplifié.
Interface utilisateur Manager-of-Managers	L'interface utilisateur Manager-of-Managers comprend l'interface graphique de Data Protector. Le logiciel est nécessaire pour l'accès aux fonctionnalités et au contrôle de l'environnement multi-cellule du Manager-of-Managers Data Protector. L'Interface utilisateur de Manager-of-Managers et l'interface utilisateur du gestionnaire sont disponibles dans une même application.
Agent de disque	Le composant Agent de disque doit être installé sur les systèmes possédant un disque à sauvegarder avec Data Protector.
Agent de support général	Le composant Agent de support général doit être installé sur les systèmes qui possèdent des périphériques de sauvegarde connectés ou ont accès à des robots de bibliothèque et qui sont gérés par Data Protector.
Récupération automatique après sinistre	Le composant Récupération automatique après sinistre doit être installé sur des systèmes sur lesquels vous voulez activer la récupération grâce à n'importe quelle méthode de récupération automatique après sinistre, ou sur des systèmes sur lesquels les images DR CD ISO pour l'EADR (Récupération après sinistre automatique avancée) ou l'OBDR (Récupération automatique après sinistre) va être configuré pour fournir une préparation automatique pour la récupération après sinistre.
Intégration SAP R/3	Le composant d'Intégration SAP R/3 doit être installé sur les systèmes possédant une base de données SAP R/3 qui sera sauvegardée avec Data Protector.

Intégration SAP MaxDB	Le composant d'Intégration SAP MaxDB doit être installé sur les systèmes possédant une base de données SAP MaxDB qui sera sauvegardée avec Data Protector.
Intégration SAP HANA	Le composant d'Intégration SAP HANA doit être installé sur les systèmes qui représentent ou constituent un appareil SAP HANA que vous voulez protéger avec Data Protector.
Intégration Oracle	Le composant d'Intégration Oracle doit être installé sur les systèmes possédant une base de données Oracle qui sera sauvegardée avec Data Protector.
MySQL Integration	Le composant d'Intégration MySQL doit être installé sur les systèmes possédant une base de données MySQL qui sera sauvegardée avec Data Protector.
Intégration de l'environnement virtuel	Le composant d'Intégration de l'environnement virtuel doit être installé sur les systèmes que vous utiliserez comme hôte de sauvegarde pour contrôler la sauvegarde et la restauration des machines virtuelles qui utilisent l'intégration de l'environnement virtuel Data Protector.
Intégration DB2	Le composant d'Intégration DB2 doit être installé sur les systèmes possédant un serveur DB2 qui sera sauvegardé avec Data Protector.
Intégration Sybase	Le composant d'Intégration Sybase doit être installé sur les systèmes possédant une base de données Sybase qui sera sauvegardée avec Data Protector.
Intégration Informix	Le composant d'Intégration Informix doit être installé sur les systèmes possédant une base de données Informix Server qui sera sauvegardée avec Data Protector.
Intégration avec MS Exchange	Le composant d'Intégration MS Exchange doit être installé sur les systèmes Microsoft Exchange Server 2007 que vous comptez sauvegarder en utilisant l'intégration Microsoft Exchange Server 2007 Data Protector ou l'intégration Microsoft Exchange Single Mailbox Data Protector. Il doit également être installé sur les systèmes Microsoft Exchange Server 2010 que vous comptez sauvegarder en utilisant l'intégration Microsoft Exchange Single Mailbox Data Protector.
Intégration avec MS Exchange Server 2010+	Le composant d'Intégration MS Exchange Server 2010+ doit être installé sur les systèmes Microsoft Exchange Server 2010 ou 2013 que vous comptez sauvegarder en utilisant l'intégration Microsoft Exchange Server 2010 Data Protector.
Intégration MS SQL	Le composant d'Intégration MS SQL doit être installé sur les systèmes possédant une base de données Microsoft SQL Server qui sera sauvegardée avec Data Protector.

Intégration MS SharePoint 2007/2010/2013	Le composant d'Intégration MS SharePoint 2007/2010/2013 doit être installé sur tous les systèmes Microsoft SharePoint Server 2007/2010/2013 qui seront sauvegardés avec Data Protector.
Intégration MS Volume Shadow Copy	Le composant d'Intégration MS Volume Shadow Copy doit être installé sur les systèmes Microsoft Server sur lesquels vous désirez lancer des sauvegardes coordonnées par Volume Shadow Copy Service.
Agent P4000 VSS	Le composant Agent VSS P4000 doit être installé sur le système d'application et le système de sauvegarde pour intégrer Solutions P4000 SAN avec Data Protector.
Agent P6000 / 3PAR SMI-S	Le composant Agent P6000 / 3PAR SMI-S doit être installé sur le système d'application et le système de sauvegarde pour intégrer Data Protector avec Famille de baies de disques P6000 EVA, ou pour intégrer Data Protector avec 3PAR StoreServ Storage.
Agent P9000 XP	Le composant Agent P9000 XP doit être installé sur le système d'application et le système de sauvegarde pour intégrer Data Protector avec Famille de baies de disque P9000 XP.
Agent 3PAR VSS	Le composant Agent 3PAR VSS doit être installé sur le serveur d'application et le serveur de sauvegarde pour intégrer Data Protector avec 3PAR StoreServ Storage quand les systèmes d'application et de sauvegarde sont des systèmes Windows et que vous voulez utiliser Volume Shadow Copy Service pour sauvegarder et restaurer vos données.
Agent EMC Symmetrix	Le composant Agent EMC Symmetrix doit être installé sur le système d'application et le système de sauvegarde pour intégrer Data Protector avec EMC Symmetrix.
Fournisseur de stockage EMC VNX	Le composant Fournisseur de stockage EMC VNX doit être installé sur le système d'application et le système de sauvegarde pour intégrer Data Protector avec EMC VNX. Le composant Fournisseur de stockage EMC VNX est un module d'extension de l'Agent Data Protector SMI-S.
Fournisseur de stockage EMC VMAX	Le composant Fournisseur de stockage EMC VMAX doit être installé sur le système d'application et le système de sauvegarde pour intégrer Data Protector avec EMC VMAX. Le composant Fournisseur de stockage EMC VMAX est un module d'extension de l'Agent Data Protector SMI-S.
Fournisseur de stockage NetApp	Le composant Fournisseur de stockage NetApp doit être installé sur le système d'application et le système de sauvegarde pour intégrer Data Protector avec NetApp Storage. Dans le cas d'une Intégration d'environnement virtuel, ce composant doit être installé uniquement sur le système de sauvegarde. Le composant Fournisseur de stockage NetApp est un module d'extension de l'Agent Data

	Protector SMI-S.
Agent de support NDMP	Le composant Agent de support NDMP doit être installé sur tous les systèmes qui sauvegarderont les données dans des lecteurs dédiés NDMP via un serveur NDMP.
Intégration Lotus	Le composant d'Intégration Lotus doit être installé sur tous les systèmes de la cellule Data Protector qui possèdent des bases de données Lotus Notes / Domino Server que vous comptez sauvegarder avec Data Protector.
Extension de restauration granulaire MS Exchange	L'Extension de restauration granulaire pour Microsoft Exchange Server de Data Protector doit être installée sur chaque système Microsoft Exchange Server pour permettre l'utilisation de la fonctionnalité restauration granulaire. Dans un environnement de groupe de disponibilité de base de données (DAG) Microsoft Exchange Server, il doit être installé en DAG sur un des systèmes Exchange Server.
Extension de restauration granulaire MS Sharepoint	L'Extension de restauration granulaire pour Microsoft SharePoint Server de Data Protector doit être installée sur le système d'administration centrale de Microsoft SharePoint Server.
Plug-in Web VMware Granular Recovery Extension Advanced GRE	Le composant VMware Granular Recovery Extension Advanced GRE Web Plug-In de Data Protector doit être installé sur le système du serveur virtuel VMware pour permettre l'utilisation de la fonctionnalité restauration granulaire des machines virtuelles VMware. L'environnement Data Protector GRE doit être configuré avant d'utiliser les plug-ins Web pour les opérations de restauration de fichier.
Agent de l'extension de restauration granulaire VMware	Le composant Agent de l'extension de restauration granulaire VMware de Data Protector doit être installé sur le système cache de montage pour permettre la restauration et la restauration granulaire des machines virtuelles VMware. Seule l'installation à distance est prise en charge.

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

Services Data Protector

Data Protector utilise les services suivants :

`Inet`	Service du client de sauvegarde
`CRS`	Service Gestionnaire de cellule

hpdp-idb	Service de la base de données interne
hpdp-idb-cp	Pooler de connexion de la base de données interne
hpdp-as	Serveur d'application

Par défaut, les services Inet et hpdp-* sont exécutés sous le compte Système local, tandis que CRS est exécuté sous le compte Administrateur.

Vous pouvez changer les informations de compte de n'importe lesquels de ces services. Cependant, vous devez garder les spécifications suivantes sur les nouveaux comptes :

Service	Ressources	Permission de ressources minimum requise par le service
CRS	*données_programme_Data_Protector* HKLM\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII	Accès complet Accès complet
Inet	Sauvegarde et Restauration Prendre possession	- -

Installation de clients Windows

Pour plus d'informations sur les plateformes et composants pris en charge par un système d'exploitation Windows en particulier, consultez https://softwaresupport.softwaregrp.com/.

Conditions préalables

Pour installer un client Windows, vous devez posséder les droits d'Administrateur. Le système Windows qui deviendra votre futur système client Data Protector doit remplir les conditions suivantes :

- Avoir suffisamment d'espace disque disponible pour le logiciel client Data Protector. Pour plus d'informations, voir Annonces sur les produits, notes sur les logiciels et références Data Protector.
- Avoir le numéro de port 5555/5565 (par défaut) disponible.
- Une recherche DNS indirecte pour résoudre le nom d'hôte est requise pour tous les composants Data Protector de la cellule Data Protector.
- Disposer d'une implémentation Microsoft opérationnelle du protocole TCP/IP. Ce protocole doit pouvoir résoudre les noms d'hôte. Le nom de l'ordinateur et le nom de l'hôte doivent être identiques.
- Assurez-vous que les droits d'utilisateur d'accès au réseau soient configurés dans la stratégie de sécurité locale de Windows pour le compte effectuant l'installation.

Limites

- En raison des restrictions de sécurité imposées par le système d'exploitation Windows, le Serveur d'installation ne peut être utilisé pour installer à distance des clients que s'ils sont du même domaine.
- Sous Windows XP Édition Familiale les clients Data Protector ne peuvent être.installés que localement.
- Lors de l'installation à distance de clients sur Windows Server 2008 ou Windows Server 2012, utilisez un des comptes suivants :
  - Un compte administrateur intégré sur le système distant. Le compte doit être activé et doit avoir le mode *Approbation administrateur désactivé.*
  - Un compte d'utilisateur de domaine

Recommandations

- Avant d'installer Data Protector, vérifiez si Microsoft Installer (MSI) 2.0 est installé sur votre système. Si une version plus ancienne est installée, il est recommandé de la mettre à niveau vers la version 2.0 avant de commencer l'installation de Data Protector. Si vous ne mettez pas MSI à niveau avant, l'Assistant d'installation de Data Protector le mettra automatiquement à niveau vers la version requise. Dans ce cas, Data Protector vous informera à propos de la mise à niveau de MSI.

  Si MSI est mis à niveau, il est hautement recommandé de redémarrer le système.

Récupération automatique après sinistre

Le composant `Automatic Disaster Recovery` doit être installé sur les systèmes sur lesquels vous voulez activer la récupération en utilisant la Récupération après sinistre automatique avancée (EADR), la Récupération automatique après sinistre (OBDR), ou la Récupération auto. système (ASR), et sur les systèmes sur lesquels l'image DR CD ISO pour EADR ou OBDR sera préparée.

Clients compatibles cluster

Des conditions préalables supplémentaires sont nécessaires pour l'installation des clients compatibles cluster. Pour plus de détails, voir Installation de clients compatibles cluster, Page 189.

Avant de démarrer la procédure d'installation, décidez quels composants vous devez installer sur votre système client. Pour connaître la liste des composants logiciels Data Protector, ainsi que leur description, voir Composants Data Protector, Page 57.

Installation en local

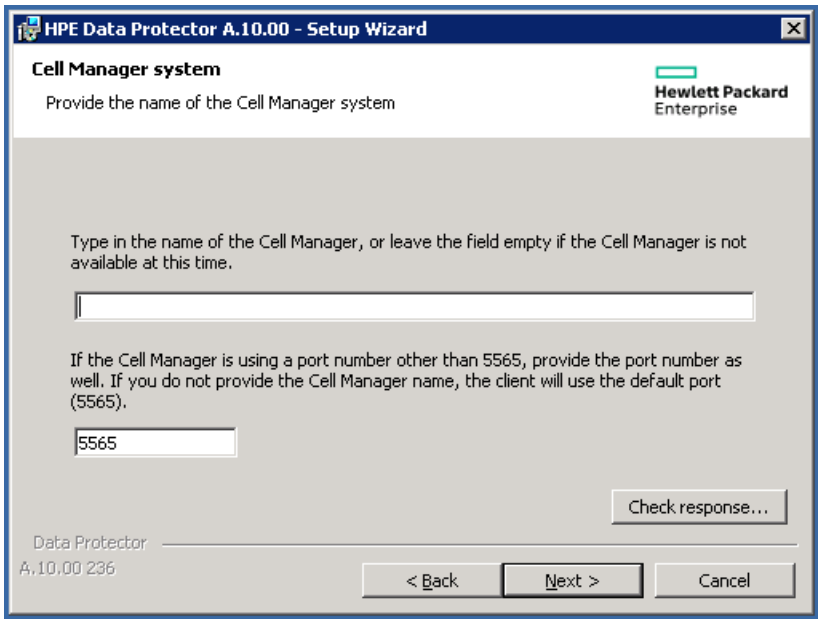
Les clients Windows peuvent être installés localement, depuis le package d'installation Windows (zip) :

1. Copiez le package d'installation téléchargé (zip) sur un système Windows et décompressez les fichiers dans un répertoire local. Exécute le fichier `setup.exe` à partir du dossier correspondant à votre plate-forme.
2. Suivez les instructions de l'assistant et lisez attentivement le contrat de licence. Cliquez sur **Suivant** pour continuer.
3. Dans la page Type d'installation, sélectionnez **Client**. Pour les clients Itanium, le type est sélectionné automatiquement.
4. Entrez le nom du Gestionnaire de cellule.

   Si votre Gestionnaire de cellule utilise un autre port que celui par défaut (5565), changez le numéro du port. Testez si le Gestionnaire de cellule est actif et utilise le port sélectionné en cliquant sur **Vérifier la réponse**.

   Cliquez sur **Suivant**.

   Choisir le Gestionnaire de cellule



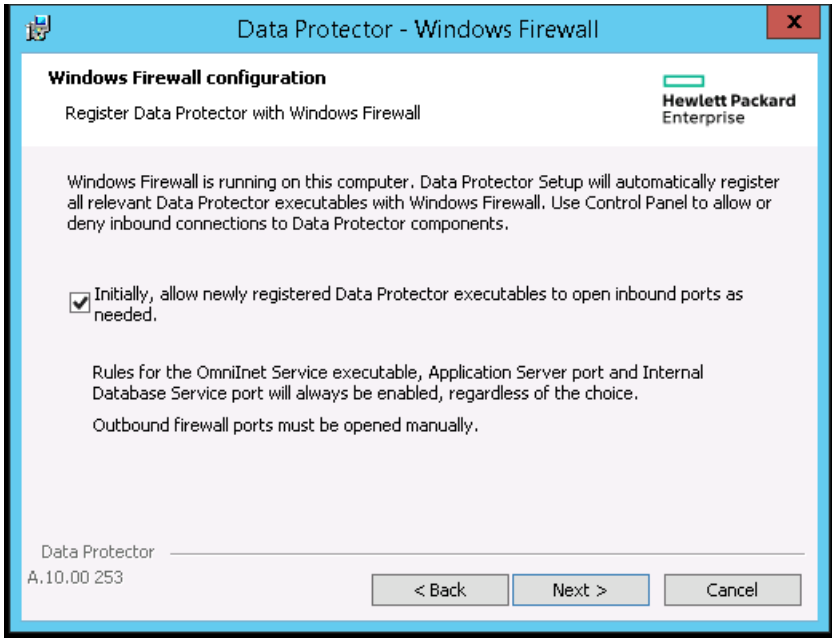
5. Cliquez sur **Suivant** pour installer Data Protector dans le dossier par défaut.

   Sinon, cliquez sur **Modifier** pour ouvrir la page Modifier le dossier de destination actuel et entrez le chemin.
6. Sélectionnez les composants Data Protector que vous voulez installer.

   Pour plus d'informations sur les autres composants Data Protector, consultez Composants Data Protector, Page 57.

   Cliquez sur **Suivant**.
7. Si Data Protector détecte Windows Firewall sur votre système, la page de configuration de Windows Firewall s'affiche. Le processus de configuration de Data Protector enregistre tous les exécutables Data Protector. 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 permettre à Data Protector d'ouvrir les ports pour le moment, ne cochez pas l'option. Pour un fonctionnement correct de Data Protector avec la version précédente des

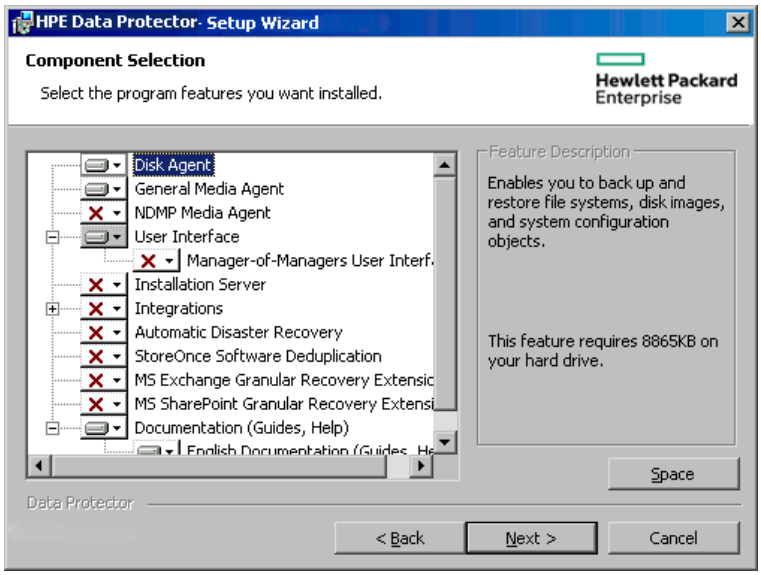
clients 10.00, les règles Data Protector dans le pare-feu Windows doivent être activées. Les règles pour l'exécutable du service OmniInet, le port du serveur d'application et le port de l'IDS seront toujours activées, indépendamment du choix effectué.



Cliquez sur **Suivant**.

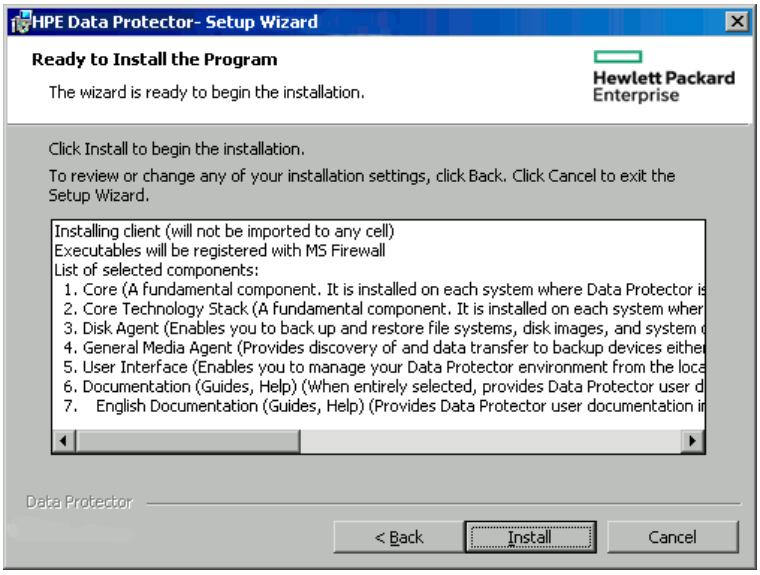
8. La liste des composants sélectionnés s'affiche. Cliquez sur **Installer** pour démarrer l'installation des composants sélectionnés.

   Écran de résumé de la sélection des composants



9. La page État de l'installation s'affiche. Cliquez sur **Suivant**.

Écran de résumé de l'installation



10. Si vous avez installé le composant `User Interface`, pour commencer à utiliser l'interface utilisateur graphique Data Protector immédiatement après l'installation, sélectionnez **Lancer l'interface utilisateur graphique de Data Protector**.

    Si vous avez installé le composant `English Documentation (Guides, Help)`, pour afficher les *Annonces sur les produits, les notes des logiciels et les références Data Protector Product* immédiatement après l'installation, sélectionnez **Ouvrir les annonces sur les produits, les notes des logiciels et les références**.
11. Cliquez sur **Terminer**.

Importation de clients installés en local

Importer signifie ajouter manuellement un système à une cellule après l'installation du logiciel Data Protector. Une fois ajouté à une cellule Data Protector, le système devient un client Data Protector.

Un client peut uniquement être membre d'une seule cellule. Si vous souhaitez déplacer un client vers une cellule différente, vous l'*exportez* tout d'abord de sa cellule actuelle puis vous l'*importez* vers la nouvelle cellule. Pour connaître la procédure si l'exportation de clients, consultez Exportation de clients d'une cellule, Page 198.

Configurer client pour importation

La procédure s'applique uniquement lorsque le nom de Gestionnaire de cellule n'est pas spécifié durant l'installation locale.

Une fois l'installation locale terminée, exécutez la commande suivante côté client :

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

Cela configure le client avec le certificat de Gestionnaire de cellule. Il s'agit d'une étape obligatoire pour les clients installés en local. Cette commande est également nécessaire pour réimporter un client supprimé.

La commande présente l'invite **y/n** permettant d'afficher ou non l'empreinte du certificat du Gestionnaire de cellule. Entrez **y** pour achever la configuration.

Si vous souhaitez configurer le client sans validation, ajoutez la commande suivante avec la commande `-accept_host` :

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

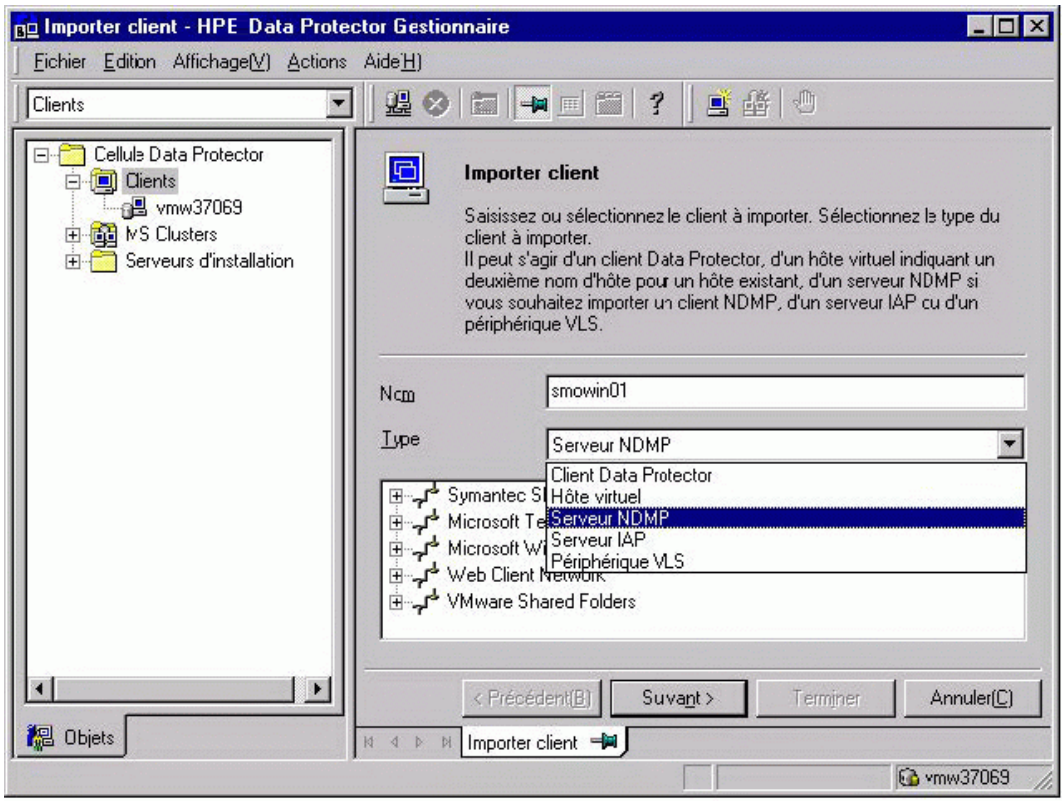
La console ne propose pas l'option **y/n** lorsque la commande `accept_host` est utilisée.

Pour importer un système client à l'aide de l'interface graphique :

Lorsque l'utilisateur sélectionne l'option **Accepter l'empreinte**, la fenêtre d'empreinte digitale n'apparaît pas et l'hôte est accepté sans confirmation de la part de l'utilisateur. Dans le cas où l'option n'est pas sélectionnée, la fenêtre d'empreinte digitale s'affiche et l'utilisateur doit accepter manuellement l'option d'empreinte.

1. Dans la liste de contexte, 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. Tapez le nom du client ou parcourez le réseau pour sélectionner le client (sur l'interface utilisateur graphique Windows uniquement) que vous souhaitez importer.

   Importer un client vers la cellule



   Si vous importez un client équipé de plusieurs cartes réseau, 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**. Entrez les informations relatives au serveur NDMP.

Si vous importez un client HP OpenVMS, tapez le nom TCP/IP du client OpenVMS dans la zone de texte `Name`.

Si vous importez un hôte virtuel Microsoft Exchange Server DAG pour l'intégration de Data Protector Microsoft Exchange Server 2010, sélectionnez **Hôte virtuel**.

Si vous importez un client pour l'intégration de l'environnement virtuel Data Protector, sélectionnez **VMware ESX(i)** pour un système de serveur VMware ESX(i) autonome, **VMware vCenter** pour un système de serveur VMware vCenter, ou **Hyper-V** pour un système Microsoft Hyper-V. Cliquez sur **Suivant** et entrez vos informations d'identification.

> **REMARQUE :**
> Pour pouvoir sauvegarder des machines virtuelles avec la méthode de sauvegarde d'image vStorage vCD, assurez-vous d'importer tous les systèmes vCenter Server utilisés par VMware vCloud Director dans la cellule Data Protector en tant que clients VMware vCenter.

4. Cliquez sur **Suivant**.
5. Cliquez sur **Terminer** pour importer le client.

Le nom du client importé s'affiche dans la zone de résultats.

Pour importer un système client à l'aide de l'interface de ligne de commande :

La commande `omnicc -import_host` est utilisée pour importer le client Data Protector et la commande `omnicc -import_cs` est utilisée pour importer le Gestionnaire de cellule extérieur. Ajoutez `-virtual` à la commande pour l'importation d'un client virtuel.

La commande présente l'invite **y/n** permettant d'afficher ou non l'empreinte du certificat du Gestionnaire de cellule. Entrez **y** pour achever la configuration. Si vous souhaitez configurer le client sans validation, ajoutez la commande avec `-accept_host`.

Spécification du Gestionnaire de cellule pendant l'installation

Si le Gestionnaire de cellule est spécifié pendant l'installation, le certificat de celui-ci est configuré sur le client dans le cadre de l'installation mais l'importation n'a pas lieu.

Pour importer un système client à l'aide de l'interface graphique ou d'une ligne de commande, consultez les sections Pour importer un système client à l'aide de l'interface graphique et Pour importer un système client à l'aide de l'interface de ligne de commande.

Gestionnaire de cellule dans une configuration MOM

Les étapes suivantes doivent être suivies pour inclure Gestionnaire de cellule dans une configuration MOM :

1. Gestionnaire de cellule doit être configuré avec le serveur MOM à l'aide de la commande suivante :

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

   Ceci configure le serveur MOM dans Gestionnaire de cellule. L'empreinte du serveur MOM est demandée et doit être acceptée par l'utilisateur.

2. Importez le Gestionnaire de cellule via l'interface utilisateur graphique MOM. Cette opération demande l'empreinte de certificat Gestionnaire de cellule que l'utilisateur doit accepter.

> **REMARQUE :**
> Gestionnaire de cellule avec différentes versions ne peut pas faire partie de la configuration MOM.

Installation locale de Serveur d'installation

Quand ajouter

Un Serveur d'installation doit être ajouté à une cellule dans les cas suivants :

- S'il est installé en tant que Serveur d'installation UNIX, 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 jusqu'à ce que Serveur d'installation ait été ajouté à cette cellule.
- S'il est installé sur un Gestionnaire de cellule, mais que vous voulez également l'utiliser pour effectuer des installations à distance dans une autre cellule. Il doit alors être ajouté à l'autre cellule (en utilisant l'interface graphique utilisateurs connectée au Gestionnaire de cellule de l'autre cellule).

A la différence d'un client, un Serveur d'installation peut être membre de plusieurs cellules. Il n'est donc pas nécessaire qu'il soit supprimé (exporté) d'une cellule pour pouvoir être ajouté (importé) dans une autre cellule.

Configuration de Serveur d'installation

Exécutez la commande suivante pour configurer l'hôte Serveur d'installation :

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

Importation de Serveur d'installation

La procédure d'importation d'un Serveur d'installation est similaire à celle d'importation d'un client. La tâche est effectuée à l'aide de l'interface graphique utilisateur Data Protector (connectée au Gestionnaire de cellule de la cellule à laquelle Serveur d'installationdoit être ajouté) en suivant les étapes suivantes :

1. Dans la liste de contexte, cliquez sur **Clients.**
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Serveur d'installations**, puis cliquez sur **Importer Serveur d'installation** pour démarrer l'assistant. Voir .
3. Entrez ou saisissez le nom du système que vous souhaitez importer. Cliquez sur **Terminer** pour importer le Serveur d'installation.

Exemple d'importation de Serveur d'installation dans Gestionnaire de cellule sous Windows/Unix/HP-UX

Si **nomhote1.societe.net** est un Gestionnaire de cellule et si **nomhote2.société.net** est un Serveur d'installation, Serveur d'installation exécute la commande suivante :

```
omnicc -secure_comm -configure_peer nomhote1.societe.net
```

```
[root@nomhote2 etc]# omnicc -secure_comm -configure_peer nomhote1.societe.net
```

```
- Utilisez l'empreinte
```

```
Pour valider manuellement le certificat !

Informations relatives au certificat :

- Nom d’hôte : nomhote1.societe.net

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

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

Souhaitez-vous continuer (o/n) ? o

Le nom d’hôte 'nomhote1.societe.net' a été correctement configuré pour une
configuration sécurisée.
```

Ensuite, au niveau du Gestionnaire de cellule, utilisez la commande suivante pour réimporter le Serveur d'installation car le certificat doit être échangé et vérifié.

```
omnicc -import_is Nomhote [-accept_host]

C:\Program Files\OmniBack\bin>omnicc -import_is nomhote2.societe.net

- Utilisez l’empreinte pour valider manuellement le certificat !

Informations relatives au certificat :

- Nom d’hôte : nomhote2.societe.net

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

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

Souhaitez-vous continuer (o/n) ? o

Importation de l'hôte réussie.
```

Connecter un périphérique de sauvegarde à un système Windows

Une fois le composant Agent de support installé, vous pouvez attacher un périphérique de sauvegarde à un système Windows grâce à la procédure suivante :

1. Trouvez des adresses SCSI (appelée *ID cibles SCSI* dans Windows) pour les lecteurs et périphériques de contrôle (robots) du périphérique de sauvegarde que vous voulez connecter. Voir Recherche des ID SCSI inutilisés sur les systèmes Windows, Page 384.
2. Configurez les `SCSI Target ID` pour les lecteurs et périphériques de contrôle (robots).. Suivant le type de périphérique, les boutons du périphérique peuvent servir à cette opération. Pour plus de détails, consultez la documentation fournie avec le périphérique.

   Pour plus d'informations sur les périphériques pris en charge, consultez https://softwaresupport.softwaregrp.com/.
3. Éteignez votre ordinateur et connectez le périphérique de sauvegarde au système.
4. Allumez en premier le périphérique, puis l'ordinateur, puis attendez que le démarrage se termine.
5. Pour vérifier que le système reconnaît bien votre nouveau périphérique de sauvegarde, dans le répertoire *répertoire_Data_Protector*`\bin`, exécutez la commande `devbra -dev`.

Vérifiez qu'un nouveau périphérique soit listé dans les résultats de la commande. Par exemple, la commande `devbra -dev` pourra vous renvoyer le résultat suivant :

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

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

  La première ligne représente les spécifications du périphérique, la seconde est le nom de fichier du périphérique.

  Le format du chemin indique qu'un lecteur de bandes DDS possède le numéro d'instance de lecteur 3 et est connecté au bus SCSI 0, ID cible SCSI 4, et LUN 0.

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

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

  La première ligne représente les spécifications du périphérique, la seconde fournit le nom de fichier du périphérique.

  Le format du chemin indique qu'un lecteur de bandes DDS est connecté au port SCSI 1, bus SCSI 0, et que le lecteur de bandes possède l'ID cible SCSI 4 et le LUN 0.

Pour charger ou décharger le lecteur de bandes natif de votre périphérique, reportez-vous à Utilisation de lecteurs bande et robotique sur systèmes Windows, Page 369.
Pour plus d'informations sur la création d'un fichier de périphérique, consultez Créer des fichiers de périphérique (adresses SCSI) sur des systèmes Windows, Page 372.

Étapes suivantes

Les composants client devraient maintenant être installés et les périphériques de sauvegarde connectés. Vous devriez être en mesure de configurer les périphériques de sauvegarde et les pools de supports. Pour plus d'informations au sujet de ces tâches de configuration, consultez l'index *Aide de Data Protector* : «configurer, périphériques de sauvegarde».

Installation de clients HP-UX

Les clients HP-UX peuvent être installés à distance grâce au Serveur d'installation pour UNIX, ou en local depuis le package d'installation UNIX (tar).

Avant de démarrer la procédure d'installation, décidez quels composants vous devez installer sur votre système client. Pour connaître la liste des composants logiciels Data Protector ainsi que leur description, consultez Composants Data Protector, Page 57.

Conditions préalables

- Le Gestionnaire de cellule et le Serveur d'installation pour UNIX devraient déjà être installés sur votre réseau. Si ce n'est pas le cas, vous pouvez trouver les instructions sur Installation du Gestionnaire de cellule et des Serveur d'installationde Data Protector, Page 26.
- Vous devez disposer soit d'un accès *root*, soit d'un compte avec des privilèges *root*.
- Une recherche DNS indirecte pour résoudre le nom d'hôte est requise pour tous les composants Data Protector de la cellule Data Protector.
- Pour HP-UX 11.11, le bouquet IPv6NCF11i ou la prise en charge TOUR/IPv6 est requis pour activer l'Internet Protocol version 6 (IPv6).

  Pour plus d'informations, voir Correctifs du système HP-UX, Page 228

Spécifications de RAM et d'espace disque des composants client Data Protector pour les systèmes UNIX

Le tableau suivant présente les spécifications de RAM et d'espace disque minimum pour les différents composants client Data Protector pour les systèmes UNIX :

Spécifications de RAM et d'espace disque

Composant système client	RAM (Mo) - [1]	Espace disque disponible (Mo) - [2]
Agent de disque	64 pour chaque (128 recommandés)	20 chacun
Agent de support		
Composants d'intégration		
Documentation en français (Guides, Aide)	Sans objet	100

Installation à distance

Installez le logiciel client depuis le Serveur d'installation pour UNIX sur les clients en utilisant l'interface graphique de Data Protector. Pour connaître la procédure d'installation du logiciel étape par étape, consultez Installation à distance, Page 95.

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

Si vous avez installé un Agent de support sur votre client, vous devez connecter physiquement le périphérique de sauvegarde au système. Pour voir si les pilotes de périphérique - qui correspondent à

[1] Les figures indiquent les spécifications uniquement pour les composants. La figure n'inclut pas l'allocation d'espace pour le système d'exploitation, le fichier d'échange ou toute autre application.
[2] Les figures indiquent les spécifications uniquement pour les composants. La figure n'inclut pas l'allocation d'espace pour le système d'exploitation, le fichier d'échange ou toute autre application.

votre périphérique - sont déjà intégrés au noyau, vérifiez la configuration de votre noyau avant de démarrer une sauvegarde.

Installation en local

Sur Serveur d'installation

Si vous n'avez pas installé de Serveur d'installation pour UNIX sur votre environnement, vous devez effectuer une installation en local à partir du package d'installation UNIX (tar). Pour connaître les étapes de l'installation locale, reportez-vous à Installation locale du serveur d'installation.

Sur les clients

Une fois l'installation en local terminée, le système client doit être importé manuellement dans la cellule. Voir Importation de clients installés en local, Page 66.

Clients compatibles cluster

Des conditions préalables et des étapes supplémentaires sont nécessaires pour l'installation de clients compatibles cluster. Pour plus de détails, voir Installation de clients compatibles cluster, Page 170.

Vérifier la configuration du noyau sur HP-UX

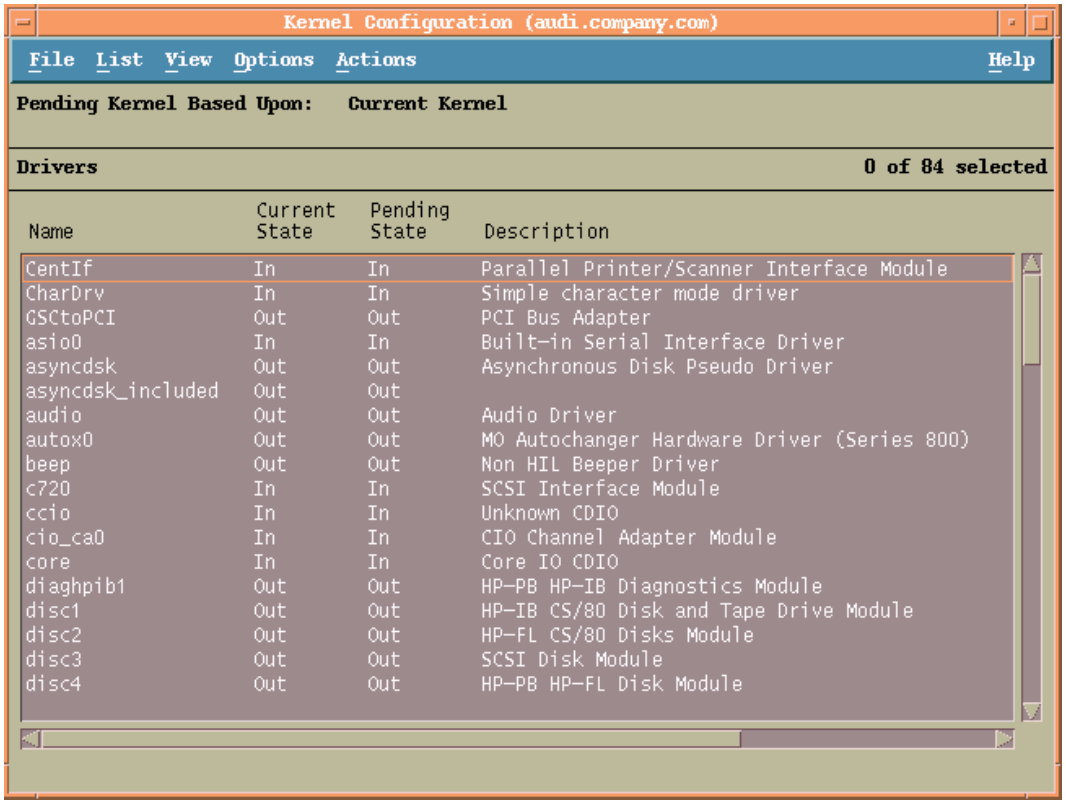
La procédure suivante décrit comment vérifier et construire la configuration de votre noyau sur HP-UX 11.x grâce à l'utilitaire *Gestionnaire d'administration système (SAM)* . Pour connaître les instructions pour construire manuellement le noyau, consultez Configuration de robotiques SCSI sur systèmes HP-UX, Page 373.

Suivez cette procédure pour construire la configuration du noyau grâce à l'utilitaire Gestionnaire d'administration système (SAM) :

1. Connectez-vous en tant qu'utilisateur `root` , ouvrez le terminal et tapez `sam`.
2. Dans la fenêtre **Gestionnaire d'administration système**, cliquez deux fois sur **Configuration du noyau**, puis sur **Pilotes**.
3. Dans la fenêtre **Configuration du noyau**, vérifiez ce qui suit :
   - Les pilotes pour les périphériques que vous utiliserez doivent être listés dans les pilotes installés. Voir Fenêtre de configuration du noyau, Page suivante. Si le pilote que vous cherchez n'est pas dans la liste, vous devez l'installer avec l'utilitaire `/usr/sbin/swinstall`. Par exemple :
     - Un pilote de lecteur de bandes est nécessaire pour les lecteurs de bandes et doit être installé si vous devez en connecter un sur le système. Par exemple, le pilote `stape` doit être utilisé pour des lecteurs de bandes SCSI génériques, comme DLT ou LTO, et le pilote `tape2` est nécessaire pour les lecteurs DDS.
     - Un pilote de passage SCSI nommé `sctl` ou `spt`, ou un pilote de robots changeurs automatiques nommé `schgr` (suivant le matériel) est requis pour contrôler les robots des bibliothèques de bandes.

       Pour plus d'informations, voir Configuration de robotiques SCSI sur systèmes HP-UX, Page 373.

Fenêtre de configuration du noyau



- L'état d'un pilote - affiché dans la colonne **État actuel** - doit être **Actif**. SI la valeur de l'état est **Inactif**, suivez cette procédure :
  a. Sélectionnez le pilote dans la liste. Cliquez sur **Actions** et sélectionnez **Ajouter un pilote au noyau**. Dans la colonne **État d'attente**, les états seront mis `In`.

     Répétez cette procédure pour chaque pilote dont l'**État actuel** est **Actif**.
  b. Cliquez sur **Actions** et sélectionnez **Créer un nouveau noyau** pour appliquer les changements, c'est-à-dire pour passer le **Noyau en attente** en **Noyau actuel**. Cette action nécessite un redémarrage du système.

Une fois tous les pilotes requis intégrés au noyau, vous pouvez connecter un périphérique de sauvegarde au système pour continuer.

Connecter un périphérique de sauvegarde à un système HP-UX

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

   Pour plus d'informations, reportez-vous à Recherche des adresses SCSI inutilisées sur les systèmes HP-UX, Page 379.
2. Configurez les adresses SCSI sur le périphérique. En général, vous pouvez le faire avec les

boutons du périphérique - suivant son type -. Pour plus de détails, consultez la documentation fournie avec le périphérique.

Pour plus d'informations sur les périphériques pris en charge, consultez https://softwaresupport.softwaregrp.com/.

3. Connectez le périphérique au système, allumez-le en premier, puis l'ordinateur, puis attendez la fin du démarrage. Les fichiers de périphérique sont généralement créés pendant le processus de démarrage.
4. Vérifiez que le système reconnaisse bien votre nouveau périphérique de sauvegarde. Utilisez l'utilitaire `ioscan` :

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

   pour voir les fichiers de périphérique listés pour chaque périphérique de sauvegarde connecté. Si le fichier de périphérique n'a pas été créé automatiquement pendant le démarrage du système, vous devrez le créer manuellement. Voir Créer des fichiers de périphérique sur des systèmes HP-UX, Page 377.

Une fois que la procédure d'installation est terminée et que les périphériques de sauvegarde ont bien été connectés au système, consultez l'index *Aide de Data Protector*: “configuration, périphériques de sauvegarde” pour plus d’informations sur la configuration de périphériques et de pools de supports ou autres tâches de configuration de Data Protector.

Installation de clients Solaris

Les clients Solaris peuvent être installés à distance grâce au Serveur d'installation pour UNIX, ou en local depuis le package d'installation UNIX (tar).

Avant de démarrer la procédure d'installation, décidez quels composants vous devez installer sur votre système client. Pour connaître la liste des composants logiciels Data Protector ainsi que leur description, consultez Composants Data Protector, Page 57.

Conditions préalables

- Lors de l'installation d'un Agent de support, assurez-vous que l'entrée suivante se trouve dans le fichier `/etc/system`:

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

- Le Gestionnaire de cellule et le Serveur d'installation pour UNIX devraient déjà être installés sur votre réseau.

  Pour obtenir des instructions, voir Installation du Gestionnaire de cellule et des Serveur d'installationde Data Protector, Page 26.

- Pour installer un client Solaris, vous n'avez pas besoin d'accès *root* ou de compte avec privilèges *root*.
- Une recherche DNS indirecte pour résoudre le nom d'hôte est requise pour tous les composants Data Protector de la cellule Data Protector.

Installation à distance

Installez le logiciel client depuis le Serveur d'installation pour UNIX sur les clients en utilisant l'interface graphique de Data Protector. Pour connaître la procédure d'installation du logiciel étape par étape, consultez Installation à distance, Page 95.

> **REMARQUE :**
> Si vous installez le composant `User Interface`, il est recommandé de mettre à niveau vos variables d'environnement avant de l'utiliser. Pour plus d'informations, reportez-vous à Configurer les variables d'environnement, Page 33.

Dès que les composants client ont été installés, le système cible devient automatiquement membre de la cellule Data Protector.

> **IMPORTANT :**
> Pour installer Data Protector dans des répertoires liés, par exemple :
>
> `/opt/omni/ -> /prefix/opt/omni/`
>
> `/etc/opt/omni/ -> /prefix/etc/opt/omni/`
>
> `/var/opt/omni/ -> /prefix/var/opt/omni/`
>
> il est recommandé de créer les liens avant l'installation et de s'assurer que les répertoires de destination existent.

> **REMARQUE :**
> Lors d'une installation ou d'une mise à niveau à distance, l'espace disque disponible dans les dossiers `/tmp` et `/var/tmp`> devrait être au moins de la taille du plus gros package à installer.

Installation en local

Si vous n'avez pas installé de Serveur d'installation pour UNIX sur votre environnement, vous devez effectuer une installation en local à partir du package d'installation UNIX (tar). Pour obtenir des instructions, voir Installation locale sur les systèmes UNIX et Mac OS X, Page 103.

Clients compatibles cluster

Des conditions préalables supplémentaires sont nécessaires pour l'installation des clients compatibles cluster. Pour plus de détails, voir Installation de clients compatibles cluster, Page 180.

Configuration post-installation

Fichiers de configuration

Une fois qu'un composant Agent de support est installé sur le système client, vous devez vérifier votre configuration pour déterminer les changements nécessaires en fonction de la plateforme et du type de périphérique que vous allez utiliser.

- Si votre système Solaris est une version 9 ou 10 mise à jour, le pilote de lecteur de bandes peut peut-être déjà prendre en charge directement votre périphérique. Pour le vérifier, utilisez la commande `strings`.

  Par exemple, pour vérifier si votre périphérique DAT-72 peut être utilisé sans configuration supplémentaire, exécutez :

  Systèmes Solaris (SPARC) :

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

  Systèmes Solaris (x86, x64) :

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

  Inspectez les résultats de la commande Si votre périphérique y est présent, vous n'avez rien à faire de plus. Dans le cas contraire, suivez les instructions ci-dessous.
- Dans le cas d'un périphérique DAT (4 mm), Ajoutez les lignes suivantes à votre 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 de données diffèrent des entrées par défaut généralement suggérées par assistance clientèle. Entrez ces lignes comme indiqué ici, ou Data Protector ne sera pas en mesure d'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 StorageWorks 12000e 48AL (C1553A), ajoutez à votre fichier `/kernel/drv/st.conf`les entrées suivantes en plus des entrées de données :

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

  Remplacez le symbole *ID* par l'adresse SCSI du chargeur automatique et mettez la valeur de son option à `5` (le bouton est situé sur le panneau arrière du périphérique) et les boutons de paramètres du DIP du périphérique à `11111001` (les boutons sont accessibles sous le chargeur automatique).

> **REMARQUE :**
> La bibliothèque StorageWorks 12000e n'a pas d'ID SCSI dédiée pour le sélecteur, mais accepte les commandes d'accès du lecteur de données et les commandes de sélecteur exécutée par la même ID SCSI. Cependant, les commandes d'accès du lecteur de données doivent être dirigées vers le SCSI lun=0 et les commandes du sélecteur vers le SCSI lun=1.

Pour tous les autres périphériques, vérifiez que le modèle `st.conf.templ` (situé dans `/opt/omni/spt`) possède les entrées requises dans le fichier `st.conf`. Ce n'est qu'un fichier modèle et il ne doit pas remplacer le fichier `st.conf`.

- Pour chaque lecteur de bandes que vous voulez utiliser, vérifiez que les lignes suivantes soient présentent dans le fichier `/kernel/drv/st.conf` et ajoutez-les si nécessaire. Remplacez le code *`ID`* par l'adresse du périphérique :

  Périphériques SCSI :

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

  Périphériques Fibre Channel :

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

  Notez que la valeur du paramètre `parent` peut changer sur votre lecteur de bandes. Pour plus d'informations, consultez la documentation de votre lecteur de bandes.

- Pour permettre le contrôle des périphériques échangeurs SCSI sous Solaris 9 et versions antérieures, vous devez installer en premier le pilote de passage SCSI, puis installer le périphérique SCSI.

  Les démarches suivantes expliquent comment installer un pilote de passage SCSI :

  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 :**
     > Lorsque vous éditez le fichier `/etc/devlink.tab`, n'utilisez pas les espaces. Faites des tabulations ([TAB]).

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

Cela va pousser les devlinks (1M) à créer un ou des liens vers les périphériques, liens dont les noms auront la forme `/dev/rsstX`, où X est le numéro cible SCSI.

3. Pour chaque échangeur SCSI que vous voulez contrôler, vérifiez que les lignes suivantes soient présentent dans le fichier `/kernel/drv/sst.conf` et ajoutez-les si nécessaire. Remplacez le *ID* par l'adresse du périphérique :

   Périphériques SCSI :

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

   Périphériques Fibre Channel :

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

   Notez que la valeur du paramètre `parent` peut changer sur votre lecteur de bandes. Pour plus d'informations, consultez la documentation de votre lecteur de bandes.

4. Entrez la commande suivante pour installer le pilote sur le système :

   ```
   add_drv sst
   ```

5. Vous êtes maintenant prêt à installer le périphérique SCSI. Avant l'installation, vous devez assigner une adresse SCSI correcte à chaque lecteur et aux robots (sélecteur) de l'échangeur. Les adresses choisies ne doivent être utilisées par un autre périphérique du système.

   Pour vérifier la configuration SCSI, exécutez la commande suivante pour éteindre le système - étape propre à Solaris (SPARC) - :

   ```
   shutdown -i0
   ```

   Puis, exécutez la commande `probe-scsi-all` à l'invite `ok` pour vérifier les adresses assignées :

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

   Dès que vous avez fini, redémarrez le système avec :

   ```
   ok boot -r
   ```

   Pour préparer votre système pour l'utilisation d'un périphérique SCSI, suivez les étapes comme montré dans l'exemple ci-dessous :

   a. Éditez `/kernel/drv/st.conf` pour configurer les paramètres du périphérique afin d'utiliser les ports SCSI assignés. Pour plus d'informations, consultez la documentation du périphérique. Ne modifiez le paramètre `tape-config-list` que si le pilote du lecteur de bandes n'est pas déjà pris en charge par votre périphérique.

   b. Éditez `/kernel/drv/sgen.conf` pour configurer les paramètres du lecteur du périphérique afin d'utiliser les ports SCSI assignés (consultez la documentation du périphérique).

   c. Éditez `/usr/kernel/drv/sgen.conf` pour paramétrer le périphérique de contrôle SCSI ADIC de sorte qu'il utilise le port SCSI 4. Ajoutez les données suivantes pour le lecteur de l'échangeur SCSI ADIC au fichier `/usr/kernel/drv/sst.conf` :

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

- Pour activer le contrôle des périphériques échangeurs SCSI sous Solaris 10 (SPARC, x86, x64), configurez le pilote intégré `sgen`, puis installez le périphérique SCSI. Suivez ces consignes :

  1. Ouvrir le fichier `/kernel/drv/sgen.conf`.

     Si le paramètre `device-type-config-list` est présent dans le fichier, ajoutez une référence pour le périphérique changeur à la ligne déjà existante. Par exemple :

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

Si le paramètre n'a pas encore été défini, ajoutez la ligne suivante au fichier :

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

2. Pour chaque échangeur SCSI que vous voulez contrôler, vérifiez que les lignes suivantes soient présentent dans le fichier `/kernel/drv/sgen.conf` et ajoutez-les si nécessaire. Remplacez le code *ID* par l'adresse du périphérique :

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

3. Vous êtes maintenant prêt à installer le périphérique SCSI. Avant l'installation, vous devez assigner une adresse SCSI correcte à chaque lecteur et aux robots (sélecteur) de l'échangeur. Les adresses choisies ne doivent être utilisées par un autre périphérique du système.

   Pour vérifier la configuration SCSI, exécutez la commande suivante pour éteindre le système - étape propre à Solaris (SPARC) - :

   ```
   shutdown -i0
   ```

   Puis, exécutez la commande `probe-scsi-all` à l'invite `ok` pour vérifier les adresses assignées :

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

   Dès que vous avez fini, redémarrez le système avec :

   ```
   ok boot -r
   ```

   Pour préparer votre système pour l'utilisation d'un périphérique SCSI, suivez les étapes comme montré dans l'exemple ci-dessous :

   a. Éditez `/kernel/drv/st.conf` pour configurer les paramètres du périphérique afin d'utiliser les ports SCSI assignés. Pour plus d'informations, consultez la documentation du périphérique. Ne modifiez le paramètre `tape-config-list` que si le pilote du lecteur de bandes n'est pas déjà pris en charge par votre périphérique.

   b. Éditez `/kernel/drv/sgen.conf` pour paramétrer le périphérique de contrôle SCSI ADIC de sorte qu'il utilise le port SCSI 4. Ajoutez les données suivantes pour le lecteur de l'échangeur SCSI ADIC au fichier `/kernel/drv/sgen.conf` :

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

Une fois que vous avez modifié les fichiers `/kernel/drv/st.conf` et `/usr/kernel/drv/sst.conf` (Solaris 9 et versions antérieures) ou le fichier `/kernel/drv/sgen.conf` (Solaris 10), vous pouvez connecter physiquement le périphérique de sauvegarde à votre système.

Connexion d'un périphérique de sauvegarde à un système Solaris

Pour connecter un périphérique de sauvegarde à un système Solaris

1. Créez un fichier `reconfigure`:

   ```
   touch /reconfigure
   ```

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

Voir https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword= pour connaître les détails sur les périphériques pris en charge.

> **REMARQUE :**
> Data Protector ne reconnait pas automatiquement les bandes nettoyantes sur un système Solaris. Si Data Protector détecte et insère une bande nettoyante dans un périphérique StorageWorks 12000e (48AL), le lecteur de bandes entre dans un état indéfini et vous pourrez avoir à redémarrer votre système. Chargez une bande nettoyante manuellement, quand Data Protector le demande.

3. Si votre système est un système Solaris (SPARC), rallumez le système et interrompez le processus de démarrage en pressant `Stop-A`.
4. Entrez la commande `probe-scsi-all` à l'invite `ok` pour vérifier que le nouveau périphérique soit bien reconnu :

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

   Puis entrez :

   ```
   ok > go
   ```

   pour continuer.
5. Le périphérique devrait maintenant fonctionner correctement. Les fichiers de périphérique doivent être dans le répertoire `/dev/rmt` pour les lecteurs et dans le répertoire `/dev` pour le périphérique de contrôle SCSI (sélecteur).

   > **REMARQUE :**
   > Sur les version 9 et antérieures de Solaris (tout spécialement la version 64 bit), les liens vers le périphérique de contrôle (sélecteur) ne sont pas toujours créés automatiquement. Sur Solaris 10, ces liens ne sont jamais créés. De ce fait, il vous faut créer des liens symboliques pour joindre les fichiers de périphérique appropriés avec `/dev/rsst`*`Num`*, où *`Num`* est un numéro de votre choix. Par exemple :
   >
   > ***Quand sst est utilisé :***
   >
   > ```
   > ln -s /devices/pci@1f,4000/scsi@3,1/sst@4,1:character /dev/rsst4
   > ```
   >
   > ***Quand sgen est utilisé :***
   >
   > ```
   > ln -s /devices/pci@1e,600000/QLGC,qla@3/sgen@8,2:changer /dev/rsst4
   > ```

   L'utilitaire Data Protector`uma` permet de vérifier le périphérique. Pour vérifier le sélecteur de l'échangeur du précédent exemple (qui utilise le port SCSI 4), entrez :

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

   Le sélecteur doit s'identifier en tant que bibliothèque de périphérique SCSI-2. La bibliothèque doit être vérifiée en la forçant à s'analyser elle-même. La commande est :

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

Assurez-vous d'utiliser des fichiers de périphérique type Berkeley : `/dev/rmt/0cbn` et non `/dev/rmt/0h`) pour le lecteur de bandes et `/dev/rsst4` pour le périphérique de contrôle SCSI (sélecteur), dans le cas présent.

Étapes suivantes

Une fois l'installation terminée et les périphériques de sauvegarde correctement connectés au client Solaris, vous pouvez obtenir plus d'informations sur la configuration des périphériques de sauvegarde, des pools de supports et des autres tâches de configuration en consultant l'index *Aide de Data Protector* : "configuration, périphériques de sauvegarde".

Installation de clients Linux

Les systèmes client Linux peuvent être installés à distance grâce au Serveur d'installation pour UNIX, ou en local depuis le package d'installation UNIX (tar).

Avant de démarrer la procédure d'installation, décidez quels composants vous devez installer sur votre système client. Pour connaître la liste des composants logiciels Data Protector ainsi que leur description, consultez Composants Data Protector, Page 57.

Conditions préalables

- Le package GNU C Library 32 bits (glibc) doit être installé sur les systèmes Linux 64 bits (x86_64).
- Le Gestionnaire de cellule et le Serveur d'installation pour UNIX devraient déjà être installés sur votre réseau.

  Pour obtenir des instructions, voir Installation du Gestionnaire de cellule et des Serveur d'installationde Data Protector, Page 26.
- L'utilitaire `rpm` doit être installé et paramétré. Les autres systèmes de package - `deb` par exemple - ne sont pas pris en charge.
- Pour installer des composants Data Protector sur un système distant, les conditions suivantes doivent être remplies :
  - Le service `inetd` ou `xinetd` doit être exécuté ou paramétré pour que Data Protector puisse le démarrer.
  - Le client doit avoir une authentification sans mot de passe ou être configuré pour `ssh`.
- Assurez-vous que le noyau prend en charge les périphériques SCSI (modules `SCSI support`, `SCSI tape support`, `SCSI generic support`). Le paramètre `Probe all LUNa on each SCSI device` est optionnel.

  Pour plus de détails sur la prise en charge SCSI du noyau Linux, consultez la documentation de votre distribution Linux ou la documentation du noyau Linux.
- Une recherche DNS indirecte pour résoudre le nom d'hôte est requise pour tous les composants Data Protector de la cellule Data Protector.

> **REMARQUE :**
> Data Protector utilise le numéro de port par défaut 5555/5565. C'est pourquoi ce port ne doit pas être utilisé par un autre programme. Certaines distributions de système d'exploitation zLinux utilisent ce port à d'autres fins.

> Si le port 5555/5565 est déjà utilisé, il est recommandé de le libérer pour Data Protector ou de changer le port par défaut pour en utiliser un de libre. Voir Changer le port Inet par défaut Data Protector, Page 354.

Récupération automatique après sinistre

Le composant `Automatic Disaster Recovery` doit être installé sur les systèmes sur lesquels vous voulez activer la récupération en utilisant la Récupération après sinistre automatique avancée (EADR), la Récupération automatique après sinistre (OBDR), ou la Récupération auto. système (ASR), et sur les systèmes sur lesquels l'image DR CD ISO pour EADR ou OBDR sera préparée.

Cluster Serviceguard

Avec les clusters Serviceguard, les agents Data Protector (Agent de disque, Agent de support) doivent être installés séparément *sur chaque nœud de cluster* (disque local) et non sur le disque partagé.

Une fois l'installation terminée, vous devez importer l'*hôte virtuel* (package application) dans la cellule en tant que client. C'est pourquoi le package application (Oracle, par exemple) doit être exécuté sur le cluster avec son *IP virtuelle*. Utilisez la commande `cmviewcl -v` pour le contrôler 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 un Agent de disque compatible OES. Cependant, certains aspects sont spécifiques à Novell OES.

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

  Veuillez noter que le nouvel Agent de disque compatible Novell OES sera installé à distance par le système client pendant la mise à niveau.
- Si vous supprimez le composant Novell OES du SLES, vous devez réinstaller le client Data Protector.

Installation à distance

Installez un système client Linux à distance en distribuant les composants Data Protector au système Linux depuis le Serveur d'installation pour UNIX grâce à l'interface graphique de Data Protector. Pour connaître la procédure de distribution du logiciel étape par étape, consultez Installation à distance, Page 95.

Dès que les composants client ont été installés, le système cible devient automatiquement membre de la cellule Data Protector.

Installation en local

Si vous n'avez pas installé de Serveur d'installation pour UNIX sur votre environnement, vous devez effectuer une installation en local à partir du package d'installation UNIX (tar). Pour obtenir des instructions, voir Installer des Serveur d'installation pour systèmes UNIX, Page 42.

Connecter un périphérique de sauvegarde à un système Linux

Une fois le composant Agent de support connecté sur le client Linux, suivez les étapes décrites ci-dessous pour connecter 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 (robots).
2. Configurez les adresses SCSI sur le périphérique. En général, vous pouvez le faire avec les boutons situés sur le périphérique - suivant son modèle -. Pour plus de détails, consultez la documentation fournie avec le périphérique.

   Pour plus d'informations sur les périphériques pris en charge, consultez https://softwaresupport.softwaregrp.com/.
3. Connectez le périphérique au système, allumez-le en premier, puis l'ordinateur, puis attendez la fin du démarrage. Les fichiers de périphérique sont créés pendant le processus de démarrage.

   Sur les systèmes Linux Red Hat Enterprise, une application - Kudzu - est lancée pendant le processus de démarrage quand un nouveau périphérique est connecté au système. Appuyez sur une touche pour démarrer l'application, puis cliquez sur le bouton `Configure`.
4. Pour vérifier que le système reconnaît votre nouveau périphérique de sauvegarde, exécutez `cat /proc/scsi/scsi` puis `dmesg |grep scsi`. Les fichiers de périphérique sont listés pour chaque périphérique de sauvegarde connecté.

   Exemples

   Pour les robots, le résultat de la commande `dmesg |grep scsi` est :

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

   et pour les lecteurs :

   ```
   Detected scsi tape st0 at scsi2, channel 0, id 5, lun 0
   ```
5. Les fichiers de périphériques sont créés dans le répertoire `/dev`. Pour vérifier si les liens vers les fichiers de périphérique ont été créés, exécutez :

   ```
   ll /dev | grep device_file
   ```

   Par exemple :

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

   Le résultat de cette commande est :

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

   `/dev/sg2` étant un lien vers le fichier de périphérique `/dev/sgc`. Cela signifie que les fichiers de périphérique que Data Protector devra utiliser sont `/dev/sgc` pour les robots et `/dev/st0` pour le

lecteur. Les fichiers de périphérique pour les robots sont `sga`, `sgb`, `sgc`,... `sgh`, et pour les lecteurs sont `st0`, `st1`,... `st7`.

Étapes suivantes

Une fois la procédure d'installation terminée et les périphériques de sauvegarde connectés au système client Linux, reportez-vous à l'entrée d'index *Aide de Data Protector* "configuration, périphériques de sauvegarde" pour obtenir des informations sur la configuration des périphériques de sauvegarde et des pools de supports ou autres tâches de configuration.

Installation de clients ESX Server

ESX Server est une version modifiée d'un système d'exploitation Linux. Pour obtenir plus d'informations sur l'installation de composants Data Protector sur les systèmes ESX Server, consultez Installation de clients Linux, Page 82.

Installation de clients IBM AIX

Les clients IBM AIX peuvent être installés à distance grâce au Serveur d'installation pour UNIX, ou en local depuis le package d'installation UNIX (tar).

Avant de démarrer la procédure d'installation, décidez quels composants vous devez installer sur votre système client. Pour connaître la liste des composants logiciels Data Protector ainsi que leur description, consultez Composants Data Protector, Page 57.

Conditions préalables

- Pour connaître la configuration requise, les exigences en termes d'espace disque, les plates-formes prises en charge et les composants Data Protector, consultez le document Annonces sur les produits, notes sur les logiciels et références Data Protector.
- Le Gestionnaire de cellule et le Serveur d'installation pour UNIX devraient déjà être installés sur votre réseau.

  Pour obtenir des instructions, voir Installation du Gestionnaire de cellule et des Serveur d'installationde Data Protector, Page 26.
- Une recherche DNS indirecte pour résoudre le nom d'hôte est requise pour tous les composants Data Protector de la cellule Data Protector.
- Avant l'installation du composant `Disk Agent`, vérifiez que portmap est opérationnel sur le système choisi. Vous devriez trouver la ligne de démarrage de portmap dans le fichier `/etc/rc.tcpip` :

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

  L'indicateur `src_running` est à 1 si le démon `srcmstr` est exécuté. Le démon `srcmstr` est le Contrôleur de ressources système (SRC). Le démon `srcmstr` crée et contrôle des sous-systèmes, gère les requêtes d'état de sous-systèmes, passe les requêtes à un sous-système et gère les messages d'erreur.

IBM HACMP Cluster

Dans l'environnement IBM High Availability Cluster Multi-Processing pour AIX, installez le composant Data Protector`Disk Agent` sur tous les nœuds de cluster. Pour obtenir plus d'informations sur comment installer Data Protector dans un environnement de cluster avec une base de données d'application compatible cluster installée, consultez Installation des clients d'intégration Data Protector, Page 113 .

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

Installation à distance

Installez le logiciel du client AIX depuis le Serveur d'installation pour UNIX sur les clients grâce à l'interface graphique de Data Protector. Pour connaître la procédure d'installation du logiciel étape par étape, consultez Installer des clients Data Protector, Page 54.

Installation en local

Si vous n'avez pas installé de Serveur d'installation pour UNIX sur votre environnement, vous devez effectuer une installation en local à partir du package d'installation UNIX (tar). Pour obtenir des instructions, voir Installer des clients Data Protector, Page 54.

Dès que les composants client ont été installés, le système cible devient automatiquement membre de la cellule Data Protector.

Connecter un périphérique de sauvegarde à un client AIX

Une fois le composant Agent de support installé sur un client AIX, procédez comme suit :

1. Éteignez l'ordinateur et connectez le périphérique de sauvegarde au bus SCSI. Vérifiez qu'aucun autre périphérique n'utilise l'adresse SCSI sélectionnée pour votre périphérique de sauvegarde.

   Pour plus d'informations sur les périphériques pris en charge, consultez https://softwaresupport.softwaregrp.com/.
2. Allumez l'ordinateur et attendez la fin du processus de démarrage. Démarrez l'outil de gestion `smit` du système AIX et vérifiez que le système ait correctement reconnu votre nouveau périphérique de sauvegarde.

   > **IMPORTANT :**
   > Utilisez `smit` pour passer à `0` la taille de bloc par défaut du périphérique (taille de bloc variable).
3. Sélectionnez les bons fichiers de périphérique dans le répertoire `/dev` et configurez votre périphérique de sauvegarde Data Protector.

> **IMPORTANT :**
> N'utilisez que des fichiers de périphérique sans rembobinage. Par exemple, sélectionnez

> `/dev/rmt0.1` au lieu de `/dev/rmt0`.

Étapes suivantes

Une fois que la procédure d'installation est terminée et que vos périphériques de sauvegarde ont bien été connectés au système AIX, consultez l'index *Aide de Data Protector*: “configuration, périphériques de sauvegarde” pour plus d’informations sur la configuration des périphériques de sauvegarde et de pools de supports ou autres tâches de configuration de Data Protector.

Installer des clients Mac OS X

Les clients Mac OS X peuvent être installés à distance grâce au Serveur d'installation pour UNIX, ou en local depuis le package d'installation d'UNIX (tar).

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

Conditions préalables

- Pour connaître la configuration requise, les exigences en termes d'espace disque, les version d'OS prises en charge et les composants Data Protector, consultez les documents Spécifications de RAM et d'espace disque, bas, Installer des clients Mac OS X, haut etInstaller des clients Mac OS X, haut.
- Voici les conditions préalables pour l'interface utilisateur Windows et les installations à distance sur le client :
  - Sur les systèmes Microsoft Windows XP Professional, Service Pack 3 doit être installé.
  - Sur les systèmes Microsoft Windows Server 2003, Service Pack 2 doit être installé.
- Le Gestionnaire de cellule et le Serveur d'installation pour UNIX devraient déjà être installés sur votre réseau.

  Pour obtenir des instructions, voir Installation du Gestionnaire de cellule et des Serveur d'installationde Data Protector, Page 26.
- Une recherche DNS indirecte pour résoudre le nom d'hôte est requise pour tous les composants Data Protector de la cellule Data Protector.

  Spécifications de RAM et d'espace disque des composants client Data Protector pour les systèmes Windows

  Le tableau suivant présente les spécifications de RAM et d'espace disque minimum pour les différents composants client Data Protector pour les systèmes Windows :

  Spécifications de RAM et d'espace disque

Composant système client	Total de RAM (MB) [1]	Espace disque disponible (Go) [2]
Interface utilisateur	512 [3]	150 [4]
Agent de disque	64 pour chaque (128 recommandés)	20 pour chaque
Agent de support		
Composants d'intégration		
Documentation en français (Guides, Aide)	Sans objet	100

Les figures indiquent les spécifications uniquement pour les composants. Par exemple, La figure «espace disque» n'inclut pas l'allocation d'espace pour le système d'exploitation, le fichier d'échange ou toute autre application.

Recommandation

- Si vous augmentez la taille de bloc par défaut, Micro Focus recommande de mettre le paramètre de noyau `kern.sysv.shmmax` (taille maximum d'un segment de mémoire partagée) à 32 MB.

Installation à distance

Installez le logiciel client Mac OS X sur les clients à partir du Serveur d'installation pour UNIX en utilisant l'interface graphique de Data Protector. Pour connaître la procédure d'installation du logiciel étape par étape, consultez Installer des clients Data Protector, Page 54.

> **REMARQUE :**
> Lors d'une installation à distance, un Serveur d'installation pour UNIX (Linux ou HP-UX) est nécessaire pour accommoder les packages (central et Agent de disque) d'installation à distance Mac OS X .

[1] Les figures indiquent les spécifications uniquement pour les composants. La figure n'inclut pas l'allocation d'espace pour le système d'exploitation, le fichier d'échange ou toute autre application.
[2] Les figures indiquent les spécifications uniquement pour les composants. La figure n'inclut pas l'allocation d'espace pour le système d'exploitation, le fichier d'échange ou toute autre application.
[3] Les spécifications de mémoire pour le système de l'interface graphique peut grandement varier en fonction du nombre d'éléments à afficher en même temps. Cette considération s'applique au pire des cas (comme développer un seul répertoire). Vous n'avez pas besoin de considérer tous les répertoires et noms de fichiers d'un client, à moins de vouloir développer tous les répertoires. Il a été montré que 2 MB de mémoire sont requis par 1000 éléments (répertoires ou noms de fichiers) à afficher en plus de la base de 50 MB. C'est pourquoi les 512 MB de RAM sont suffisants pour afficher le maximum de noms de fichiers.
[4] En ce qui concerne l'espace disque, gardez en tête que le fichier d'échange est capable d'atteindre à lui tout seul environ 3 fois la mémoire physique.

Installation en local

Si vous n'avez pas installé de Serveur d'installation pour UNIX sur votre environnement, vous devez effectuer une installation en local à partir du package d'installation d'UNIX (tar). Pour obtenir des instructions, voir Installer des clients Data Protector, Page 54.

Dès que les composants client ont été installés, le système cible devient automatiquement membre de la cellule Data Protector.

Installation de clients OpenVMS HP

La procédure d'installation pour les clients OpenVMS doit être effectuée 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 de support général et l'Interface utilisateur (en ligne de commande uniquement) de Data Protector sur les systèmes OpenVMS 7.3-2/IA64 8.2-1. Vous pouvez également installer le composant d'intégration Oracle sur les systèmes OpenVMS 7.3-2 ou plus récents. Pour plus d'informations sur les autres composants Data Protector, consultez Composants Data Protector, Page 57.

Pour plus d'informations sur les périphériques pris en charge ainsi que les versions des plateformes OpenVMS et leurs restrictions, problèmes connus et solutions, consultez Annonces sur les produits, notes sur les logiciels et références Data Protector.

Pour plus d'informations propres à OpenVMS, consultez *Notes de mise à jour d'OpenVMS*, que vous pouvez trouver dans le répertoire par défaut des documents d'aide d'OpenVMS. Par exemple `SYS$COMMON:[SYSHLP]DPA0800.RELEASE_NOTES`:

Conditions préalables

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

- Assurez-vous que le protocole de transport TCP/IP de est bien opérationnel.
- Configurez les fonctionnalités TIMEZONE sur votre système en exécutant la commande `SYS$MANAGER:UTC$TIME_SETUP.COM`.
- Connectez-vous au compte `SYSTEM` du système OpenVMS. Notez que vous devez posséder les permissions appropriées.
- Vérifiez que vous avez accès au package d'installation (zip/tar) Data Protector contenant le package d'installation du client HP OpenVMS.
- Une recherche DNS indirecte pour résoudre le nom d'hôte est requise pour tous les composants Data Protector de la cellule Data Protector.

Procédure d'installation

La procédure d'installation peut être effectuée depuis le package d'installation Windows (zip) Data Protector.

Pour installer un client Data Protector sur un système OpenVMS

1. Si vous avez déjà le fichier d'installation PCSI, rendez-vous directement à Installer des clients Data Protector, Page 54. Pour obtenir le fichier d'installation PCSI, extrayez le package d'installation sur un serveur OpenVMS et copiez-le dans l'emplacement voulu. Vous pouvez également utiliser un ftp depuis un système Windows.
2. Exécutez la commande suivante :

   ```
   $ PRODUCT INSTALL DP /SOURCE=device:[directory]
   ```

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

   Exemple

   ```
   The following product has been selected: AXPVMS DP A08.00-xx Layered Product Do
   you want to continue? [YES]
   ```
4. Choisissez les composants logiciel que vous voulez installer. Choisissez par défaut pour que l'Agent de disque, l'Agent de support général et l'Interface utilisateur soient installés. Vous pouvez également sélectionner chaque composant individuellement.

   L'installation vous demandera de choisir les options, s'il y en a, pour chaque produit sélectionné et pour chaque produit qui pourrait être installé pour remplir les conditions des dépendances.

   Exemple

   ```
   HP IA64VMS DP A08.00-xx: HP OpenVMS IA64 Data Protector V8.00
   COPYRIGHT HEWLETT-PACKARD COMPANY 2013
   Do you want the defaults for all options? [YES] NO
   Do you wish to install Disk Agent for this client node?
   [YES] YES
   Do you wish to install Media Agent for this client node?
   [YES] YES
   Do you wish to install Command Language Interface for this client node?
   [YES] YES
   Do you wish to install Oracle Integration Agent for this client node?
   [YES] YES
   Do you want to review the options?
   [NO] YES
   HP IA64VMS DP X08.00-xx: HP OpenVMS IA64 Data Protector V8.00 [Installed]
   Do you wish to install Disk Agent for this client node?
   YES
   Do you wish to install Media Agent for this client node?
   YES
   Do you wish to install Command Language Interface for this client node?
   YES
   Do you wish to install Oracle Integration Agent for this client node?
   ```

```
[YES] YES
Are you satisfied with these options?
[YES] YES
```

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

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

La structure de répertoire sera créée automatiquement et les fichiers seront placés dans cet arbre de répertoires.

Les procédures des commandes de démarrage et de fermeture de Data Protector seront placées dans

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

Quatre fichiers sont toujours présents sur un client OpenVMS, et un cinquième fichier n'existe que si vous choisissez l'option Interface en ligne de commande. Voici les cinq fichiers en question :

- `SYS$STARTUP:OMNI$STARTUP.COM` est la procédure de commande qui démarre Data Protector sur ce nœud.
- `SYS$STARTUP:OMNI$SYSTARTUP.COM` est la procédure de commande qui définit le nom logique d'`OMNI$ROOT`. Tout nom logique requis par ce client peut être ajouté à cette procédure de commande.
- `SYS$STARTUP:OMNI$SHUTDOWN.COM` est la procédure de commande qui ferme Data Protector sur ce nœud.
- `OMNI$ROOT:[BIN]OMNI$STARTUP_INET.COM` est la procédure de commande utilisée pour démarrer le processus `TCP/IP INET`, qui exécutera alors les commandes envoyées par le Gestionnaire de cellule
- `OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COM` est la procédure de commande qui définit les symboles nécessaire pour appeler l'Interface en ligne de commande de Data Protector. Elle ne sera sur le système que si vous choisissez l'option Interface en ligne de commande pendant l'installation.

  Exécutez cette procédure de commande depuis les procédures `login.com` pour tous les utilisateurs qui utiliseront l'interface en ligne de commande. Plusieurs noms logiques sont définis dans cette procédure et sont nécessaires pour exécuter correctement les commandes de l'interface en ligne de commande.

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. Assurez-vous que vous pouvez vous connecter depuis le client OpenVMS à tous les alias TCP/IP possibles pour le Gestionnaire de cellule.
8. Importez le client OpenVMS dans la cellule Data Protector en utilisant l'interface graphique de Data Protector.

Un compte nommé `OMNIADMIN` est créé pendant l'installation. Le service `OMNI` est exécuté sous ce compte.

Le répertoire de connexion de 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 de chaque processus exécutant la requête, le nom de l'image Data Protector utilisée et les options de la requête.

Les erreurs inattendues sont consignées dans le `DEBUG.LOG` de ce répertoire.

> **REMARQUE :**
> Sur OpenVMS 8.3 et sur les versions plus récentes, l'installation de Data Protector affiche le message suivant :
>
> ```
> %PCSI-I-CANNOTVAL, cannot validate [PATH]HP-AXPVMS-DP-A0800
> -XXX-1.PCSI;1 -PCSI-I-NOTSIGNED, product kit
> is not signed and therefore has no manifest file
> ```
>
> Pour éviter cette alerte, exécutez la commande d'installation du produit en utilisant `/OPTION=NOVALIDATE_KIT`.

Installation dans un environnement de cluster

Si vous utilisez un disque système commun, vous n'avez besoin d'installer le logiciel client qu'une fois. Cependant, la procédure `OMNI$STARTUP.COM` doit être exécutée pour que chaque nœud puisse être utilisable en tant que 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 définir un client pour le nom d'alias si vous utilisez un disque système commun pour le cluster. Une fois le client alias défini, vous n'avez pas besoin de configurer les nœuds clients individuels. Vous pouvez choisir soit une définition de client, soit une définition d'alias pour exécuter vos sauvegardes et vos restaurations dans un cluster. En fonction de votre configuration, la sauvegarde ou la restauration peut ou ne peut pas utiliser de chemin direct vers votre lecteur de bandes ou votre bibliothèque de bandes.

Configuration de l'Agent de disque

L'Agent de disque Data Protector sous OpenVMS prend en charge les volumes de disque montés `FILES-11 ODS-2` et `ODS-5`. Il n'est pas nécessaire de configurer l'Agent de disque OpenVMS. Il y a, cependant, certains points à garder en tête quand vous mettez en place les spécifications de sauvegarde qui vont l'utiliser. Ces points sont décrits ci-dessous :

- Les spécifications de fichier entrées dans l'interface graphique ou passées à l'interface en ligne de commande doivent utiliser la syntaxe d'UNIX. Par exemple :

  ```
  /disk/directory1/directory2/.../filename.ext.n
  ```

  - La chaîne doit commencer par un slash, suivi du disque, des répertoires et du nom de fichier, séparés par des slashs.
  - Ne placez pas de virgule après le nom du disque.
  - Un point doit être utilisé avant le numéro de version au lieu d'un point-virgule.
  - Les spécifications de fichiers OpenVMS ne respectent pas la casse, à l'exception des fichiers résidant sur des disques `ODS-5`.

Exemple

Une spécification de fichier OpenVMS de :

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

doit être transmise à Data Protector sous cette forme :

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

> **REMARQUE :**
> Il n'y a pas de numéro de version implicite. Vous devez toujours spécifier le numéro de version, et uniquement la version spécifiée d'un fichier sera sauvegardée.
>
> Pour certaines options qui autorisent les caractères génériques, le numéro de version peut être remplacé par un astérisque '*'.
>
> Pour inclure toutes les versions d'un fichier dans une sauvegarde, vous devez toutes les sélectionner dans l'interface graphique, ou inclure les spécifications de fichier sous l'option `-only` dans l'interface en ligne de commande, en utilisant des caractères génériques pour indiquer le numéro de version, comme ceci :
>
> `/DKA1/dir1/filename.txt.*`

Configuration de l'Agent de support

Il est recommandé de configurer les périphériques de votre système OpenVMS avec l'aide de la documentation du matérielle et d'OpenVMS. Les pseudo-périphériques de la bibliothèque de bandes doivent être créés en premier avec SYSMAN, comme ceci :

```
$ RUN SYS$SYSTEM:SYSMAN

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

où :

- `c` = K pour les bibliothèques de bandes SCSI connectées en direct.
- `a` = A, B, C, …le caractère de l'adaptateur pour le contrôleur SCSI.
- `n` = le numéro d'unité du robot de contrôle de la bibliothèque de bandes.

> **REMARQUE :**
> Cette séquence de commandes doit être exécutée après le démarrage d'un système.

Pour les bibliothèques de bandes SAN attachées, le nom des lecteurs de bandes et du robot devrait apparaître automatiquement sous OpenVMS une fois que les périphériques SAN ont été configurés conformément aux directives SAN.

Si vous installez un jukebox pour une utilisation avec Data Protector, il vous faut vérifier que le matériel fonctionne correctement avant de le configurer dans Data Protector. Il est possible d'utiliser Media Robot Utility (MRU), disponible auprès de Hewlett-Packard, pour vérifier le matériel.

> **REMARQUE :**
> Vous pouvez généralement utiliser l'interface graphique de Data Protector pour configurer manuellement ou automatiquement ces périphériques.

> Cependant, certains vieux modèles de bibliothèques de bandes et toute bibliothèque de bande connectée à des contrôleurs HSx ne peuvent être configurés automatiquement. Utilisez les méthodes de configuration manuelles pour ajouter ces périphériques à Data Protector.

Agent de support dans un cluster

Quand vous devez gérer des périphériques attachés à des systèmes de cluster :

1. Configurez chaque lecteur et chaque bibliothèque de bandes pour qu'ils soient accessibles depuis chaque nœud.
2. Ajoutez le nom de nœud à la fin du nom de périphérique pour différencier les périphériques.
3. Pour les périphériques à bandes, configurez un `Device Lock Name` commun sous `Devices/Properties/Settings/Advanced/Other`.

Exemple

Dans un cluster avec des nœuds A et B, un TZ89 est connecté au nœud A et un MSCP au nœud B. Configurez un périphérique nommé `TZ89_A` qui a le nœud A en client, et configurez un périphérique nommé `TZ89_B` qui a le nœud B en client. Le nom de périphérique verrouillé commun des deux périphériques est `TZ89`. Data Protector peut désormais utiliser les périphériques depuis n'importe quel chemin, puisqu'il ne s'agit que d'un seul périphérique. Si vous lancez une sauvegarde sur le nœud B en utilisant `TZ89_A`, Data Protector déplace les données du nœud B vers le périphérique du nœud A. Si vous lancez une sauvegarde sur le nœud B en utilisant `TZ89_B`, le serveur OpenVMS MSCP déplace les données du nœud B vers le périphérique du nœud A.

> **REMARQUE :**
> Pour les lecteurs de bandes d'un cluster servis par MSCP, pour tous les lecteurs de bandes connectés via un contrôleur HSx et pour tous les lecteurs de bandes connectés via Fibre Channel, suivez les directives pour les configurations SAN indiquées dans l'index *Aide de Data Protector* :

Interface en ligne de commande

Avant d'être en mesure d'utiliser l'interface en ligne de commande de Data Protector sur OpenVMS, vous devez exécuter la procédure d'installation des commandes CLI suivante :

```
$ @OMNI$ROOT:[BIN]OMNI$CLI_SETUP.COM
```

Pour obtenir une description des commandes CLI disponibles, consultez *Guide de référence de l'interface de ligne de commande Data Protector*.

Intégration Oracle

Une fois l'intégration Oracle installée et configurée comme indiqué dans le *Guide d'intégration Data Protector*, vérifiez que l'entrée `-key Oracle8` est présente dans `OMNI$ROOT:[CONFIG.CLIENT]omni_info`. Par exemple :

```
-key oracle8 -desc “Oracle Integration” -nlsset 159 -nlsId 12172 -flags 0x7 -ntpath
““ -uxpath ““ -version 9.00
```

Si l'entrée n'est pas présente, copiez-la à partir de `OMNI$ROOT:[CONFIG.CLIENT]omni_format`. Si vous ne le faites pas, l'intégration Oracle n'apparaîtra pas comme étant installée sur le client OpenVMS.

Étapes suivantes

Pour plus d'informations au sujet des tâches de configuration supplémentaires, consultez l'index *Aide de Data Protector* :

Installation à distance

Cette section décrit la procédure utilisée pour distribuer le logiciel Data Protector aux clients en utilisant le Serveur d'installation (installation ou mise à niveau à distance).

Distribuez le logiciel aux clients à l'aide de l'interface utilisateur Data Protector. L'installation du client sur plusieurs plateformes est prise en charge.

Conditions préalables

- Pour les conditions préalables et les recommandations sur l'installation, consultez la section qui décrit la procédure d'installation pour le client qui vous intéresse. La liste des références se trouve dans Installer des systèmes clients Data Protector , Page 54 et Installer des intégrations, Page 55.
- Pour obtenir des informations sur les plateformes et les composants Data Protector pris en charge, et sur les critères en matière d'espace disque, consultez https://softwaresupport.softwaregrp.com/ et Installation à distance, haut.
- À ce stade, le Gestionnaire de cellule et le ou les Serveur d'installation devraient déjà être installés sur votre réseau.
- Pour avoir une installation à distance propre, le Serveur d'installation pour Windows doit être dans un répertoire partagé afin d'être visible sur le réseau.
- ***Windows 2012 :*** Pour installer à distance un système Windows 2012, effectuez l'une des mesures suivantes :
  Configurez l'utilisateur de domaine qui est également l'administrateur de l'hôte distant (`omniinetpasswd -inst_srv_user`) sur l'**Serveur d'installationhôte** du . L'installation à distance est démarrée sous ce compte et la connexion à l'hôte distant est établie sans intervention supplémentaire de l'utilisateur.

  OU

  Bloquez les services suivants dans le pare-feu de l'**hôte distant**.
  - Gestionnaire de services à distance (RPC)
  - Gestionnaire de services à distance (RPC-EPMAP)

  OU

  Coupez le RPC/TCP (côté client) sur l'**Serveur d'installationhôte** du .

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control`

  `DWORD SCMApiConnectionParam = 0x80000000`

  Combinez la valeur du registre `SCMApiConnectionParam` avec la valeur du masque `0x80000000`.

  > **REMARQUE :** le système n'a pas besoin d'être redémarré.

Configurer le pare-feu pour une installation à distance réussie

Au cours de l'installation d'un nouveau client Data Protector, ou de la mise à jour d'un ancien client Data Protector, à l'aide du Serveur d'installation, l'agent d'installation démarre sur l'ordinateur distant. Le Serveur d'installation se connecte alors à l'agent par le port de la cellule Data Protector (5555/5565 par défaut). Cependant, si le pare-feu Windows, ou tout logiciel tiers de pare-feu, est en cours d'exécution sur le client, la connexion ne pourra être établie, et l'installation sera un échec. Les instructions suivantes résolvent ce problème :

- Configurez le pare-feu Windows pour autoriser une connexion via un port particulier.
- Pour le pare-feu Windows : si l'option omnirc `OB2FWPASSTHRU` est activée sur le Serveur d'installation, l'agent d'installation va automatiquement s'enregistrer auprès du pare-feu Windows et l'installation continuera normalement.

Recommandations

- ***Systèmes UNIX :*** Pour des raisons de sécurité, il est recommandé d'utiliser un shell sécurisé pour une installation à distance de Data Protector. Lorsque le SSH est configuré, l'authentification se fera sans mot de passe, ou les informations d'identification seront demandées à l'utilisateur.

  Pour utiliser un shell sécurisé, installez et paramétrez OpenSSH sur le client et sur le Serveur d'installation. Si votre clé privée est cryptée, installez et paramétrez keychain sur le Serveur d'installation. Voir Installer des clients Data Protector, Page 54.

> **REMARQUE :**
> Vous ne pouvez pas distribuer un logiciel à des clients situés dans une autre cellule Data Protector. Cependant, si vous avez un Serveur d'installation indépendant, vous pouvez l'importer dans plus d'une cellule. Vous pouvez alors distribuer le logiciel dans les différentes cellules grâce à l'interface graphique connectée à chaque Gestionnaire de cellule.

- ***Comptes administrateur :*** Pour utiliser des utilisateurs locaux qui appartiennent au groupe Administrateurs de l'hôte distant, quand l'hôte distant a l'UAC activé, effectuez l'une des opérations suivantes sur l'**hôte distant** :

  Désactivez le Contrôle de compte d'utilisateur (UAC)

  > **REMARQUE :** le système a besoin d'être redémarré.

  OU

  Configurez la valeur du registre :

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

  > **REMARQUE :** le système n'a pas besoin d'être redémarré.

Installation à distance avec un shell sécurisé

L'installation d'un shell sécurisé vous aide à protéger votre client et le Serveur d'installation en installant les composants Data Protector de manière sécurisé. Un haut niveau de protection est obtenu grâce à :

- L'authentification sécurisée des utilisateurs de Serveur d'installation pour le client via un mécanisme de paires de clés publique-privée.
- L'envoi de packages d'installation cryptés par le réseau.

> **REMARQUE :**
> L'installation d'un shell sécurisé est prise en charge uniquement sur les systèmes UNIX.

Paramétrer OpenSSH

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

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

   Si le package OpenSSH ne fait pas partie de la distribution de votre OS, téléchargez OpenSSH sur http://www.openssh.org et installez-le sur le client Data Protector et sur le Serveur d'installation.

   Vous pouvez également utiliser le shell sécurisé de HP-UX, sur les systèmes HP-UX.

   > **REMARQUE :**
   > L'emplacement par défaut de l'installation du shell sécurisé est `/opt/ssh`

2. Sur le Serveur d'installation, exécutez `ssh-keygen` pour générer une paire de clés publique-privée. Gardez 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.à.d. protégée par une phrase de passe), vous devez configurer keychain sur le Serveur d'installation (pour plus de détails, consultez Installer des clients Data Protector, Page 54).

   Pour obtenir des informations sur `ssh-keygen`, consultez 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 généralement le répertoire de base de l'utilisateur `root`.

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

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

      `ssh_install_directory` `/ssh/etc/ssh_config`

      Ce fichier sera utilisé par la commande `ssh`.

   b. ***Sur le client***

      `ssh_install_directory` `/ssh/etc/sshd_config`

      Cette commande sera utilisée par le démon `ssh` (`sshd`).

   Veuillez noter que ces deux fichiers doivent être synchronisés.

   > **REMARQUE :**
   > La version par défaut du protocole SSH est SSH2.

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

   `ssh_install_directory` `/ssh/sbin/sshd`

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

   `ssh root@client_host`

   où *client_host* doit être un nom DNS valide, comme par exemple :

   `ssh root@client1.company.com`

Mettre en place keychain

Keychain est un outil qui élimine la nécessité de fournir manuellement une phrase passe quand vous décryptez une clé privée. Il n'est nécessaire que si la clé privée est cryptée.

Pour mettre en place keychain :

1. Téléchargez keychain sur le depuis http://www.gentoo.org/proj/en/keychain/index.xmlServeur d'installation.
2. Ajoutez les deux lignes suivantes à `$HOME/.profile` :

   Systèmes HP-UX et Solaris :

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

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

   Systèmes Linux :

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

   `. $HOME/.keychain/'hostname'-sh`
3. Sur le Serveur d'installation, mettez l'option omnirc `OB2_ENCRYPT_PVT_KEY` à `1`. Pour plus d'informations sur les options de `omnirc`, reportez-vous au *Guide de dépannage Data Protector*.

   Si l'installation du shell sécurisé ne peut être effectuée parce que l'exécution de sa commande échoue, une alerte sera donnée. Cependant, l'installation continuera à utiliser la méthode d'installation à distance standard de Data Protector.

Étapes suivantes

Une fois OpenSSH et keychain en place, ajoutez des clients à la cellule avec l'interface graphique comme décrit dans Installer des clients Data Protector, Page 54 ou exécutez la commande `ob2install` pour utiliser l'interface en ligne de commande. Pour plus d'informations sur les commandes CLI et leurs paramètres, consultez *Guide de référence de l'interface de ligne de commande Data Protector*.

> **REMARQUE :**
> Si l'installation du shell sécurisé ne peut être effectuée parce que l'exécution de sa commande échoue, une alerte sera donnée. Cependant, l'installation continuera à utiliser la méthode d'installation à distance standard de Data Protector.

Ajouter des clients à la cellule

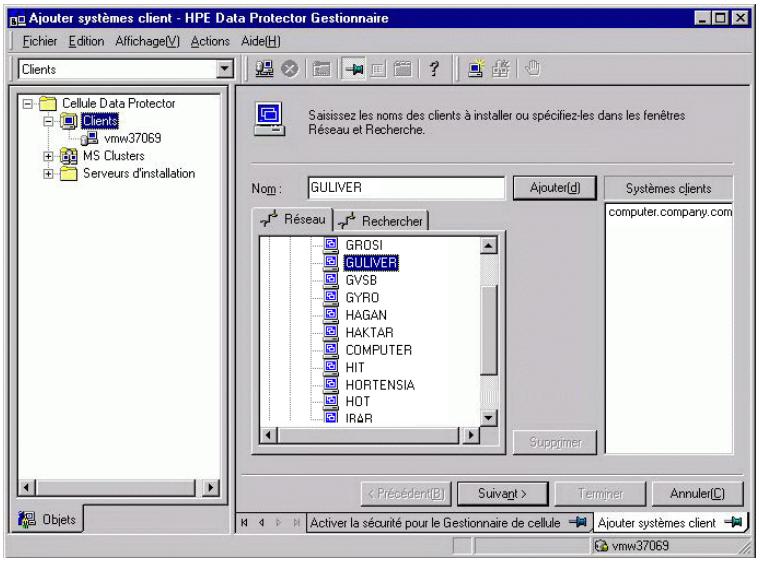
Pour distribuer le logiciel Data Protector aux clients qui ne sont pas encore dans la cellule Data Protector

1. Démarrez le GUI Data Protector en cliquant sur **Démarrer** > **Programmes** > **Data Protector** > **Data Protector Manager**.

   > **REMARQUE :**
   > Pour plus d'informations sur l'interface utilisateur graphique de Data Protector, consultez leL'interface graphique de Data Protector, Page 24 et le*Aide de Data Protector*.

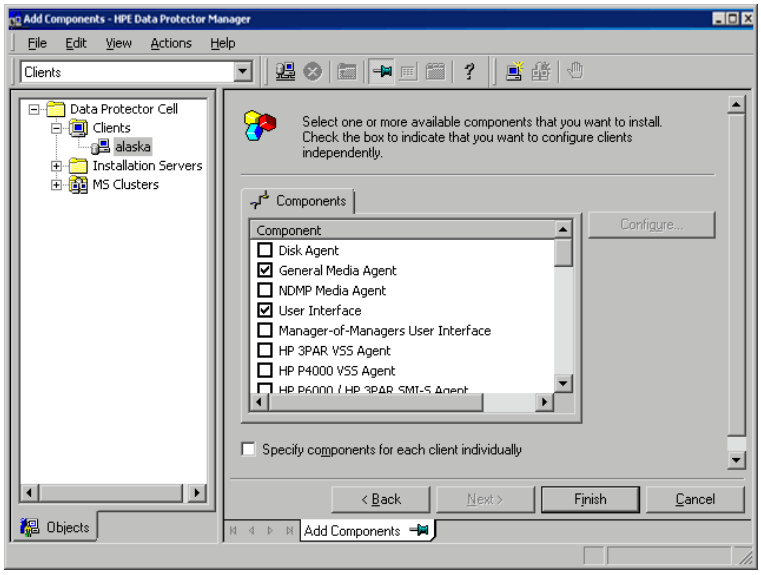
2. Dans Data Protector Manager, affichez le contexte **Clients**.
3. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Clients** puis cliquez sur **Ajouter clients**.
4. Si vous avez plus d'un Serveur d'installation configuré, sélectionnez la plateforme des clients que vous voulez installer (UNIX ou Windows) et le Serveur d'installation à utiliser pour installer ces clients. Cliquez sur **Suivant**.
5. Tapez les noms des clients ou cherchez les clients (uniquement sur l'interface graphique de Windows) que vous voulez installer comme montré dans Installer des clients Data Protector, Page 54. Cliquez sur **Suivant**.

   Sélectionner des clients

6. Sélectionnez les composants Data Protector que vous souhaitez installer comme montré dans Installer des clients Data Protector, Page 54. Notez que vous ne pouvez sélectionner qu'un type d'Agent de support. Voir Composants Data Protector, Page 57.

Sélectionner des composants



7. Pour changer le compte d'utilisateur par défaut et le répertoire cible (uniquement sur Windows) de l'installation, cliquez sur **Options**.
8. Si vous sélectionnez plus d'un client et que vous voulez installer des composants différents sur chaque client, cliquez sur **Spécifier individuellement les composants pour chaque client**, puis cliquez sur **Suivant**. Sélectionnez les composants que vous souhaitez installer sur chaque client.
9. Cliquez sur **Suivant**.
10. Cliquez sur **Terminer** pour démarrer l'installation.
11. Pendant l'installation, renseignez les données qui vous seront demandées (nom d'utilisateur, mot de passe, et domaine si vous êtes sous Windows) pour accéder au système spécifique du client et cliquez sur **OK**.

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

> **REMARQUE :**
> Avant de commencer à utiliser l'interface graphique de Data Protector sur le système client, ajoutez un utilisateur de ce système au groupe d'utilisateur Data Protector approprié. Pour connaître la procédure et pour obtenir des descriptions des droits d'utilisateur disponibles, consultez *Aide de Data Protector*.

Dépannage

Une fois l'installation à distance terminée, vous pouvez redémarrer les procédures d'installation échouées grâce à l'interface graphique en cliquant sur **Actions** puis **Redémarrer les clients échoués.**. Si l'installation échoue à nouveau, consultez Dépannage des problèmes d'installation et de mise à jour, Page 323.

Ajouter des composants aux clients

Vous pouvez installer des composants logiciels Data Protector supplémentaires sur les clients existants et le Gestionnaire de cellule. Les composants peuvent être ajoutés à distance ou en local. Pour l'installation locale, voir Modification des composants logiciels Data Protector, Page 238

Conditions préalables

Le correspondant Serveur d'installation doit être disponible.

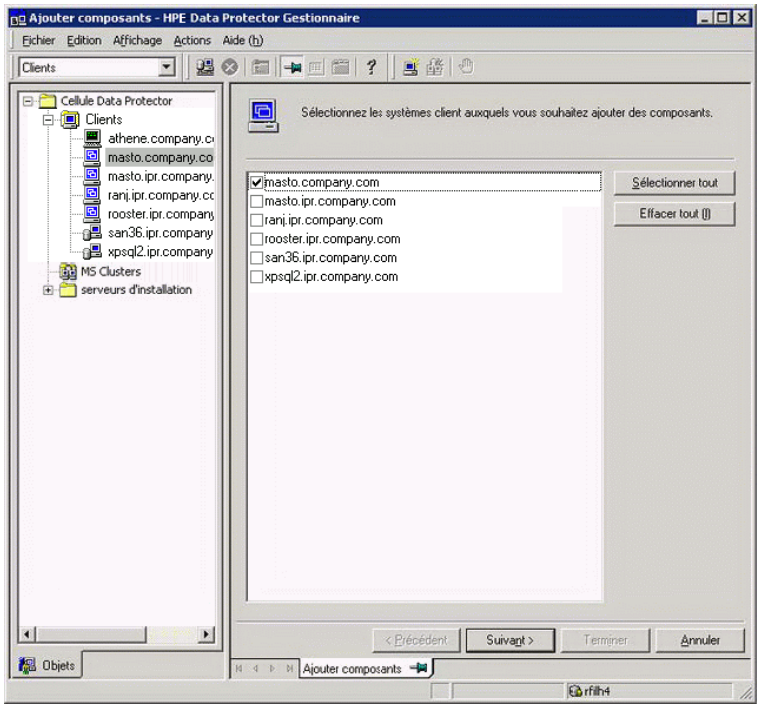
Clients Serviceguard

Dans l'environnement de cluster Serviceguard, assurez-vous que le nœud auquel vous voulez ajouter des composants soit actif.

Pour distribuer les logiciels Data Protector aux clients de la cellule Data Protector

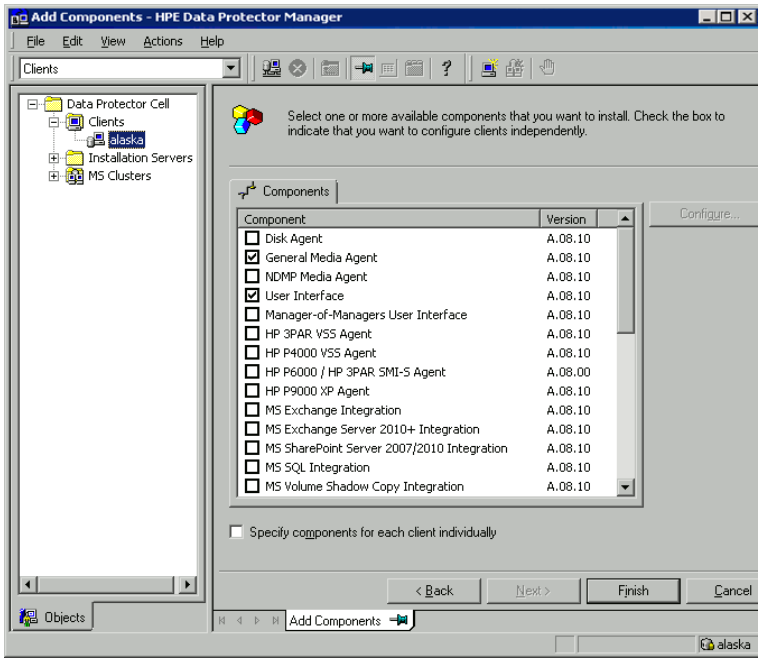
1. Dans Data Protector Manager, affichez le contexte **Clients**.
2. Dans la fenêtre de navigation, développez Clients, cliquez avec le bouton droit sur un client, puis cliquez sur **Ajouter des composants**.
3. Si vous avez plus d'un Serveur d'installation configuré, sélectionnez la plateforme des clients auxquels vous voulez ajouter des composants (UNIX ou Windows) et le Serveur d'installation à utiliser pour installer ces composants. Cliquez sur **Next**.
4. Sélectionnez les clients auxquels vous voulez installer des composants comme montré dans Sélectionner des clients, Page suivante. Cliquez sur **Next**.

Sélectionner des clients



5. Sélectionnez les composants Data Protector que vous souhaitez installer comme montré dans Installer des clients Data Protector, Page 54. Notez que vous ne pouvez sélectionner qu'un type d'Agent de support. Voir Composants Data Protector, Page 57.

Sélectionner des composants



Si vous sélectionnez plus d'un client et que vous voulez installer des composants différents sur chaque client, cliquez sur **Spécifier individuellement les composants pour chaque client**, puis cliquez sur **Next**. Sélectionnez les composants pour chaque client indépendamment.

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

Installation locale sur les systèmes UNIX et Mac OS X

Si vous n'avez pas de Serveur d'installation pour UNIX installé sur votre réseau, ou si pour une raison quelconque vous ne pouvez pas installer un système client à distance, les clients Data Protector peuvent être installés en local à partir du package d'installation UNIX (tar).

Avant de démarrer la procédure d'installation, décidez quels composants vous devez installer sur votre système client. Pour connaître la liste des composants logiciels Data Protector ainsi que leur description, consultez Composants Data Protector, Page 57.

> **REMARQUE :**
> Les clients Windows XP Édition Familiale et HP OpenVMS peuvent être installés en local. L'installation à distance n'est pas prise en charge.

Conditions préalables

- Pour connaître la configuration requise, les exigences en termes d'espace disque, les plates-formes prises en charge, les processeurs et les composants Data Protector, consultez le document Annonces sur les produits, notes sur les logiciels et références Data Protector.
- Vous devez disposer des droits d'accès `root` sur chaque système cible.
- Un shell POSIX (`sh`) doit être utilisé pour l'installation.

> **REMARQUE :**
> Vous pouvez également utiliser la procédure suivante pour mettre à niveau en local les clients UNIX. Le script détectera une installation précédente et vous proposera de faire une mise à niveau.

Procédure d'installation

Pour installer en local des clients UNIX et Mac OS X

1. Copiez le package d'installation Data Protector téléchargé (tar) sur le système HP-UX ou Linux et extrayez les fichiers vers un répertoire local.
2. Depuis le répertoire `LOCAL_INSTALL`, exécutez la commande `omnisetup.sh`.

   La syntaxe de la commande est la suivante :

   `omnisetup.sh [-source` *`directory`*`] [-server` *`name`*`] [-install` *`component_list`*`]`

   où :

   - *répertoire* est l'emplacement où le package d'installation est extrait. Si l'emplacement n'est pas spécifié, le répertoire actuel sera utilisé.

- *nom* est le nom d'hôte complet du Gestionnaire de cellule de la cellule vers laquelle vous voulez importer le client. Si le nom n'est pas spécifié, le client ne sera pas automatiquement importé dans la cellule.

  > **REMARQUE :**
  > Dans le cas d'une mise à niveau du client situé sur le Gestionnaire de cellule ou le Serveur d'installation, vous n'avez pas besoin de spécifier `-install` *`component_list`*. Dans ce cas-là, l'installation va sélectionner les composants qui ont été installés sur le système avant la mise à niveau sans rien demander.

- *liste_des_composants* est une liste de codes de composants à installer séparés d'une virgule. Il ne faut pas d'espace. Si le paramètre `-install` n'est pas spécifié, vous serez informé de l'installation de chaque composant disponible sur le système.

  > **REMARQUE :**
  > Dans le cas d'une mise à niveau du client, l'installation sélectionnera les composants qui ont été installés sur le système avant le démarrage de la mise à niveau, sans rien demander.

  La liste des composants est présentée dans le tableau ci-dessous. La liste exacte des composants dépend de la disponibilité sur un système donné. Pour avoir la description des composants, consultez Composants Data Protector, Page 57.

Data Protector component codes

Code du 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
`oracle8`	Intégration Oracle
`mysql`	MySQL Integration
`postgresql`	Intégration de PostgreSQL
`vepa`	Intégration de l'environnement virtuel
`sybase`	Intégration Sybase

Code du composant	Composant
sap	Intégration SAP R/3
sapdb	Intégration SAP MaxDB
saphana	Intégration SAP HANA
db2	Intégration DB2
emc	Agent EMC Symmetrix
smisa	Agent P6000 / 3PAR SMI-S
ssea	Agent P9000 XP
emcvnx	Fournisseur de stockage EMC VNX
emcvmax	Fournisseur de stockage EMC VMAX
netapp	Fournisseur de stockage NetApp
StoreOnceSoftware	Déduplication du logiciel StoreOnce.
autodr	Récupération automatique après sinistre
docs	Documentation en français (Guides, Aide)

Exemple

L'exemple ci-dessous vous montre comment installer les composants `Disk Agent`, `General Media Agent`, `User Interface` et `Informix Integration` sur un client qui sera automatiquement importé dans la cellule avec Gestionnaire de cellule`computer.company.com`:

```
./omnisetup.sh -server computer.company.com -installda,ma,cc,informix
```

3. L'installation vous informe si elle a réussi 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 être installé.

   Le composant `CORE-INTEG` est installé la première fois qu'un composant logiciel d'intégration est sélectionné pour être installé ou réinstallé.

Lancer une installation depuis le disque dur

Copiez le package d'installation sur votre ordinateur et exécutez l'installation ou la mise à jour des clients UNIX et Mac OS X depuis le disque dur, en copiant au moins les répertoires `hpux/DP_DEPOT` et `LOCAL_INSTALL`.

> **REMARQUE :**
> Le dépôt Linux ne prend pas en charge les installations en local. Vous devez copier le dépôt HP-UX, même sur les systèmes Linux/

Par exemple, si vous copiez les packages d'installation dans `/var/dp80`, les répertoires doivent être des sous-répertoires de `/var/dp10`:

```
# pwd

/var/dp80

# ls

DP_DEPOT

LOCAL_INSTALL
```

Une fois les données copiées sur le disque dur, passez dans le répertoire `LOCAL_INSTALL` et exécutez la commande suivante :

```
omnisetup.sh [-server name] [-install component_list]
```

Par exemple :

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

Veuillez noter que si vous copiez le répertoire `DP_DEPOT` dans un répertoire différent (par exemple à cause de problèmes d'espace disque), l'option `-source` est aussi nécessaire.

Étapes suivantes

Si vous n'avez pas spécifié le nom du Gestionnaire de cellule pendant l'installation, le client ne sera pas importé dans la cellule. Dans ce cas-là, il est recommandé de l'importer avec l'interface graphique de Data Protector. Pour plus d'informations au sujet de tâches de configuration supplémentaires, consultez *Aide de Data Protector*.

Installation d'un Agent de support pour utiliser la bibliothèque ADIC/GRAU ou la StorageTek Library

Data Protector fournit des stratégies de bibliothèques dédiées ADIC/GRAU et StorageTek ACS utilisées pour configurer une bibliothèque ADIC/GRAU ou une bibliothèque StorageTek ACS pour servir de périphérique de sauvegarde Data Protector. Il est nécessaire d'installer un Agent de support Data Protector (l'Agent de support général ou l'Agent de support NDMP) sur chaque système physiquement connecté à un lecteur d'une bibliothèque ADIC/GRAU ou StorageTek. De plus, pour les configurations multi-hôtes, vous devez installer un Agent de support Data Protector sur les systèmes qui contrôlent les robots de la bibliothèque ADIC/GRAU ou StorageTek. Veuillez noter qu'une configuration multi-hôtes est une configuration où la bibliothèque et le lecteur ne sont pas connectés au même ordinateur.

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

REMARQUE :
Vous devez disposer de licences spéciales, selon le nombre de lecteurs et d'emplacements utilisés dans la bibliothèque StorageTek. Pour plus d'informations, reportez-vous à Data Protector Licensing, Page 279.

Connexion de lecteurs de bibliothèque

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

Pour plus d'informations au sujet des bibliothèques ADIC/GRAU ou STK prises en charge, consultez https://softwaresupport.softwaregrp.com/.

Pour plus d'informations sur comment connecter physiquement un périphérique de sauvegarde à un système, consultez Installer des clients Data Protector, Page 54 et la documentation livrée avec la bibliothèque ADIC/GRAU ou StorageTek.

Pour plus d'informations sur comment connecter physiquement un périphérique de sauvegarde à un système Windows pris en charge, consultez Installer des clients Data Protector, Page 54 et la documentation livrée avec la bibliothèque ADIC/GRAU ou StorageTek.

Préparer les clients Data Protector pour l'utilisation d'une bibliothèque ADIC/GRAU

Les opérations suivantes servent à configurer une bibliothèque ADIC/GRAU, et doivent être suivies avant d'installer un logiciel d'Agent de support :

1. Si le serveur DAS est basé sur OS/2, avant de configurer un périphérique de sauvegarde ADIC/GRAU Data Protector, créez ou mettez 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 qui peut contrôler des robots de bibliothèque doit être défini dans ce fichier.

   Chaque client DAS est identifié par un nom de client unique (sans espace), par exemple `DP_C1`. Par exemple, le contenu du fichier `C:\DAS\ETC\CONFIG` devrait ressembler à cela :

   ```
   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 avec un Agent de support Data Protector installé qui nécessite un accès aux robots de bibliothèque ADIC/GRAU DAS, éditez le fichier `omnirc`et paramétrez les options suivantes :

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

3. Vous devez trouver le type de configuration (statique ou dynamique) de la stratégie d'allocation des emplacements de votre bibliothèque ADIC/GRAU. Pour plus d'informations sur comment

vérifier le type de stratégie d'allocation utilisée, consultez le *Manuel de référence AMU*.

La stratégie statique possède un emplacement désigné pour chaque volser, alors que la stratégie d'allocation dynamique assigne les emplacements aléatoirement. Vous devez configurer Data Protector en fonction de la stratégie utilisée.

Si la stratégie d'allocation est statique, vous devez ajouter l'option omnirc suivante au système qui contrôle les robots de bibliothèque :

```
OB2_ACIEJECTTOTAL = 0
```

> **REMARQUE :**
> Cela concerne HP-UX et Windows.

Si vous avez des questions concernant la configuration de votre bibliothèque ADIC/GRAU, contactez votre support technique ADIC/GRAU local ou consultez votre documentation ADIC/GRAU.

Installer un Agent de support pour utiliser une bibliothèque ADIC/GRAU

Conditions préalables

Les conditions préalables à l'installation suivantes doivent être remplies avant d'installer un Agent de support sur un système :

- La bibliothèque ADIC/GRAU doit être configurée et opérationnelle. Consultez la documentation fournie avec la bibliothèque ADIC/GRAU.
- Data Protector doit être installé et configuré. Pour obtenir des instructions, voir Installation du Gestionnaire de cellule et des Serveur d'installationde Data Protector, Page 26.
- Le serveur DAS doit être opérationnel.

  Pour contrôler la bibliothèque ADIC/GRAU, le logiciel DAS est requis. Chaque client DAS doit avoir un logiciel client DAS installé. Chaque action liée à un support ou un périphérique initiée par Data Protector va d'abord du client DAS au serveur DAS. Puis il passe par la partie interne (Unité de gestion AMU - AML) de la bibliothèque ADIC/GRAU qui contrôle les robots et déplace ou charge les supports. Une fois l'action terminée, le serveur DAS répond au client DAS. Consultez la documentation fournie avec la bibliothèque ADIC/GRAU.
- Les informations suivantes doivent être obtenues avant d'installer l'Agent de support :
  - Le nom d'hôte du serveur DAS (une application qui tourne sous un hôte OS/2).
  - La liste des lecteurs disponibles avec le nom DAS correspondant. Les noms de lecteur obtenus doivent être utilisés pour configurer les lecteurs ADIC/GRAU dans Data Protector.

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

    ```
    dasadmin listd2 client
    dasadmin listd client
    ```

    où *`client`* est le client DAS dont les lecteurs réservés doivent être affichés.

La commande `dasadmin` peut être appelée depuis le répertoire `C:\DAS\BIN` de l'hôte OS/2, ou depuis le répertoire où le logiciel client DAS a été installé, dans le cas où il aurait été installé sur d'autres systèmes. 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 des zones d'insertion/éjection disponibles dans la configuration graphique d'AMS (Logiciel de gestion AML) sur un hôte OS/2 :

  1. Démarrer la configuration depuis le menu `Admin > Configuration`.
  2. Cliquez deux fois sur l'icône **Unité I/O** pour ouvrir la fenêtre **Configuration-EIF**, puis cliquez sur le champ **Intervalles logiques**. Les zones d'insertion/éjection disponibles sont listées dans la zone de texte.

     > **REMARQUE :**
     > Un périphérique de bibliothèque Data Protector ne peut gérer qu'un 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 besoin de ces données ultérieurement pour configurer les zones d'insertion/éjection de la bibliothèque Data Protector.

- Une liste des fichiers de périphérique UNIX des lecteurs, si vous voulez installer un Agent de support sur un système UNIX.

  Exécutez la commande système `ioscan -fn` sur votre système pour afficher l'information requise.

  Pour plus d'informations sur les fichiers de périphériques UNIX, consultez Installer des clients Data Protector, Page 54.

- Une liste des adresses SCSI des lecteurs, si vous voulez installer un Agent de support sur un système Windows. Par exemple, `scsi4:0:1:0`.

  Pour plus d'informations sur les adresses SCSI, consultez Installer des clients Data Protector, Page 54.

Procédure d'installation

La procédure d'installation se déroule de la sorte :

1. Distribuez un composant Agent de support aux clients, grâce à l'interface graphique de Data Protector et au Serveur d'installation. Voir Installer des clients Data Protector, Page 54.
2. Installez la bibliothèque ADIC/GRAU :
   - Sur un système Windows, opérez de la sorte :
     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. Ils figurent sur le support d'installation ou dans le répertoire `C:\DAS\AMU\` sur le AMU-PC.)
     b. Copiez également ces trois fichiers dans le répertoire *%SystemRoot%*`\system32`.
     c. Copiez `Portinst` et `Portmapper service` dans le client DAS. (Ces éléments requis font

partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU. Vous pouvez les trouver sur le support d'installation.)

d. Dans le panneau de configuration, allez à `Administrative Tools, Services` et démarrez `portinst` pour installer `portmapper`. Le client DAS doit être redémarré pour pouvoir exécuter le service `portmapper` .

e. Après le redémarrage du système, vérifiez si `portmapper` et les deux services `rpc services` sont lancés. Dans le Panneau de configuration, allez dans **Outils administratifs, Services** et vérifiez l'état des services.

- Sur un système HP-UX, copiez la bibliothèque partagée `libaci.sl` dans le répertoire `/opt/omni/lib`. Vous devez disposer de permissions suffisantes pour accéder au répertoire. Assurez-vous que la bibliothèque partagée a lu et exécuté toutes les permissions (root, groupe et autres). La bibliothèque partagée `libaci.sl` fait partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU. Vous pouvez la trouver sur le support d'installation.

- Sur un système AIX, copiez la bibliothèque partagée `libaci.o` dans le répertoire `/usr/omni/lib`. Vous devez disposer de permissions suffisantes pour accéder au répertoire. Assurez-vous que la bibliothèque partagée a lu et exécuté toutes les permissions (root, groupe et autres). La bibliothèque partagée `libaci.o` fait partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU. Vous pouvez la trouver sur le support d'installation.

Vous devriez maintenant avoir votre matériel connecté et votre logiciel DAS installé correctement.

À partir de l'emplacement des commandes administratives Data Protector par défaut, exécutez la commande `devbra -dev` pour vérifier si les lecteurs de bibliothèque sont reliés correctement à votre système.

Regardez si les lecteurs de bibliothèque et leurs fichiers de périphérique correspondants apparaissent dans la liste.

Étapes suivantes

Une fois un agent de support installé et la bibliothèque ADIC/GRAU physiquement reliée au système, consultez l'index *Aide de Data Protector* : "configuration, périphériques de sauvegarde" afin d'obtenir des instructions sur les tâches de configuration avancée, comme la configuration des périphériques de sauvegarde et des pools de supports.

Préparer les clients Data Protector pour l'utilisation d'une bibliothèque StorageTek

Conditions préalables

Les conditions préalables à l'installation suivantes doivent être remplies avant d'installer un Agent de support :

- La bibliothèque StorageTek doit être configurée et opérationnelle. Consultez la documentation fournie avec la bibliothèque StorageTek.

- Data Protector doit être installé et configuré. Voir Installation du Gestionnaire de cellule et des Serveur d'installationde Data Protector, Page 26.
- Les informations suivantes doivent être obtenues avant d'installer un logiciel d'Agent de support :
  - Le *nom d'hôte* 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 obtenues doivent être utilisées pour configurer les lecteurs StorageTek dans Data Protector. Pour afficher cette liste, connectez-vous à l'hôte où ACSLS est en cours d'exécution et exécutez la commande suivante :

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

    Vous devrez entrer le type du terminal et attendre l'invite de commande. À 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 et de spécifications de format CAP ACS. Pour afficher cette liste, connectez-vous à l'hôte où ACSLS est en cours d'exécution et exécutez la commande suivante :

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

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

    ```
    ACSSA> query cap all
    ```

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

    ```
    ACS CAP: ID:#,#,# - (ACS num, LSM num, CAP num)
    ```
  - Une liste des fichiers de périphérique UNIX des lecteurs, si vous voulez installer un Agent de support sur un système UNIX.

    Exécutez la commande système `ioscan -fn` sur votre système pour afficher l'information requise.

    Pour plus d'informations sur les fichiers de périphériques UNIX, consultez Installer des clients Data Protector, Page 54.
  - Une liste des adresses SCSI des lecteurs, si vous voulez installer un Agent de support sur un système Windows. Par exemple, `scsi4:0:1:0`.

    Pour plus d'informations sur les adresses SCSI, consultez Installer des clients Data Protector, Page 54.
- Assurez-vous que les lecteurs qui vont être utilisés pour Data Protector soient bien dans l'état `online`. Si l’état d’un lecteur n'est pas `online`, changez-le à l'aide de la commande suivante sur l'hôte ACSLS : `vary drive drive_id online`
- Assurez-vous que les CAP qui vont être utilisés pour Data Protector soient bien dans l'état `online` et en mode de fonctionnement `manual`.

  Si un CAP n'est pas dans l'état `online`, changez l'état avec la commande suivante :

  ```
  vary cap cap_id online
  ```

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

```
set cap manual cap_id
```

Installer un Agent de support pour utiliser une bibliothèque StorageTek

Pour installer un Agent de support pour utiliser une bibliothèque StorageTek

1. Distribuez un composant Agent de support aux clients grâce à l'interface graphique de Data Protector et au Serveur d'installation pour systèmes UNIX. Voir Installer des clients Data Protector, Page 54.
2. Démarrez le démon `ssi` ACS pour chaque client ACS :

   Systèmes Windows :

   Installez le service `LibAttach`. Pour plus d'informations, consultez la documentation ACS. Vérifiez que, lors de la configuration du service `LibAttach`, le nom d'hôte ACSLS correct est saisi. Au terme d'une configuration réussie, les services `LibAttach` sont lancés automatiquement. Ils seront également lancés automatiquement après chaque redémarrage.

   Systèmes HP-UX, Solaris et Linux :

   Exécutez la commande suivante :

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

   Systèmes AIX :

   Exécutez la commande suivante :

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

   > **REMARQUE :**
   > Après avoir installé le service `LibAttach`, vérifiez si le répertoire `libattach\bin` a été ajouté automatiquement au chemin d'accès du système. Si tel 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. À partir de l'emplacement des commandes administratives Data Protector par défaut, exécutez la commande `devbra -dev` pour vérifier si les lecteurs de bibliothèque sont reliés correctement à votre système.

   Regardez si les lecteurs de bibliothèque et leurs fichiers de périphérique/adresses SCSI correspondants apparaissent dans la liste.

Étapes suivantes

Lorsqu'un Agent de support est installé et que la bibliothèque StorageTek est physiquement connectée au système, consultez l'index : *Aide de Data Protector* index: “configuration, périphériques de sauvegarde” pour plus d’informations sur la configuration de périphériques de sauvegarde et de pools de supports.

Chapitre 4: Installation des clients d'intégration Data Protector

Les intégrations Data Protector sont des composants logiciels qui vous permettent de lancer des sauvegardes en ligne des applications de base de données - comme Oracle Server ou Microsoft Exchange Server - avec Data Protector. Les intégrations ZDB Data Protector sont des composants logiciel qui vous permettent de lancer des sauvegardes sans pause et des restaurations instantanées grâce à des baies de disques, comme Famille de baies de disques P6000 EVA.

Les systèmes qui exécutent les applications de base de données sont appelés **clients d'intégration** ; les systèmes qui utilisent des baies de disques ZDB pour sauvegarder et stocker des données sont appelés **clients d'intégration ZDB**. La procédure d'installation de ces clients sur les systèmes Windows ou Unix est la même que pour tout autre client, pour peu que le composant logiciel correspondant ait bien été sélectionné (par exemple, le composant `MS Exchange Integration` pour sauvegarder une base de données Microsoft Exchange Server, le composant `P6000 / 3PAR SMI-S Agent` pour ZDB et IR avec Famille de baies de disques P6000 EVA ou StoreServ Storage, et ainsi de suite).

Conditions préalables

- Pour connaître la configuration requise, les exigences en termes d'espace disque, les plates-formes prises en charge, les processeurs et les composants Data Protector, consultez le document Annonces sur les produits, notes sur les logiciels et références Data Protector.
- Il vous faut une licence pour utiliser l'intégration Data Protector avec une application base de données (sauf pour l'intégration VSS). Pour plus d'informations sur les licences, voir Data Protector Structure et licences de produit, Page 308.
- Le Gestionnaire de cellule et le Serveur d'installation (optionnel, pour une installation à distance) devraient déjà être installés sur votre réseau.

  Pour obtenir des instructions, voir Installation du Gestionnaire de cellule et des Serveur d'installationde Data Protector, Page 26.

Avant de démarrer la procédure d'installation, décidez quels autres composants logiciel Data Protector vous voulez installer sur votre client en même temps que le composant d'intégration. Pour connaître la liste des composants logiciels Data Protector , ainsi que leur description, voir Composants Data Protector, Page 57.

Veuillez noter que dans les cas présentés ci-dessous, vous devez installer les composants Data Protector suivants :

- Le composant `Disk Agent` pour pouvoir sauvegarder les données du système de fichiers avec Data Protector. Vous pouvez utiliser l'Agent de disque dans les situations suivantes :
  - Pour lancer une sauvegarde du système de fichiers pour les données importantes qui *ne peuvent pas* être sauvegardées avec une sauvegarde d'application de base de données.
  - Pour lancer un test de sauvegarde du système de fichiers d'un serveur d'application de base de données (par exemple, Oracle Server, ou Microsoft SQL Server). Il vous faut tester la sauvegarde de système de fichiers *avant* de configurer l'intégration Data Protector avec une application de base de données et résoudre la communication et autres problèmes liés à l'application et à Data Protector.

  - Pour lancer une sauvegarde sans pause du système de fichiers ou des images disque.
  - Pour restaurer depuis un support de sauvegarde vers un système d'application en LAN en cas d'intégrations SAP R/3 ZDB.

- Le composant `User Interface` pour avoir accès à l'interface graphique Data Protector et à l'interface en ligne de commande de Data Protector sur le client d'intégration de Data Protector.
- Le composant `General Media Agent` si vous avez des périphériques de sauvegarde connectés au client d'intégration de Data Protector. Sur les clients Data Protector utilisés pour accéder au lecteur dédié NDMP via le serveur NDMP, `NDMP Media Agent` est requis.

Les clients d'intégration peuvent être installés à distance grâce au Serveur d'installation pour Windows ou UNIX, ou en local depuis le package d'installation Windows ou UNIX (zip/tar).

Pour plus d'informations sur les clients d'intégration particuliers, consultez la section correspondante ci-dessous :

- Clients Microsoft Exchange Server, Page 116
- Clients Microsoft SQL Server, Page 123
- Clients Microsoft SharePoint Server, Page 123
- Clients de Microsoft Volume Shadow Copy Service, Page 127
- Clients Sybase Server, Page 128
- Clients Informix Server, Page 128
- Clients SAP R/3, Page 129
- Clients SAP MaxDB, Page 129
- Clients SAP HANA Appliance, Page 129
- Clients Oracle Server, Page 130
- Clients MySQL, Page 130
- Clients PostgreSQL, Page 131
- Clients IBM DB2 UDB, Page 131
- Clients Lotus Notes/Domino Server, Page 131
- Clients VMware, Page 132
- Clients Microsoft Hyper-V, Page 140
- Clients NDMP Server, Page 141
- Solutions P4000 SAN clients, Page 142
- Famille de baies de disques P6000 EVA clients, Page 142
- Famille de baies de disque P9000 XP clients, Page 148
- 3PAR StoreServ Storage clients, Page 154
- Clients EMC Symmetrix, Page 154
- Baies de stockage non HPE, Page 159

Une fois les clients d'intégration installés, Micro Focus vous recommande d'activer les appels de commandes Data Protector depuis n'importe quel répertoire en ajoutant les localisations des commandes à la variable d'environnement correspondante sur chaque client. Les procédures décrites dans la documentation de Data Protector considèrent que la valeur des variables a été étendue. Les

localisations des commandes sont listées dans la page de référence `omniintro` que vous pouvez retrouver dans *Guide de référence de l'interface de ligne de commande Data Protector* et sur la page man relative à `omniintro`.

Après l'installation, consultez également le *Guide d'intégration Data Protector*, le *Guide de l'administrateur Data Protector Sauvegarde avec temps d'indisponibilité nul*, ou le *Guide d'intégration Data Protector Sauvegarde avec temps d'indisponibilité nul* pour configurer les clients d'intégration Data Protector.

Installation à distance

Installez le logiciel client depuis le Serveur d'installation sur les clients en utilisant l'interface graphique de Data Protector. Pour connaître la procédure d'installation du logiciel étape par étape, consultez Installation à distance, Page 95.

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

Installation en local

Si vous n'avez pas installé de Serveur d'installation correspondant au système d'exploitation sur votre environnement, vous devez effectuer une installation en local à partir du package d'installation de Windows ou d'UNIX (zip/tar), suivant la plate-forme sur laquelle vous installez le client.

Si vous ne choisissez pas un Gestionnaire de cellule pendant l'installation, le système client doit être importé manuellement dans la cellule après l'installation en local. Voir Importation de clients installés en local, Page 66.

Installer des intégrations compatibles cluster

Les clients d'intégration compatible cluster Data Protector doivent être installés en local, depuis le package d'installation, sur chaque nœud de cluster. Pendant l'installation en local d'un client, installez, en plus des autres composants logiciels client, les composants logiciels d'intégration appropriés (comme `Oracle Integration` ou `P6000 / 3PAR SMI-S Agent`).

Vous pouvez également installer une application de base de données compatible cluster et un Agent ZDB sur le Data Protector de Gestionnaire de cellule. Sélectionnez le composant logiciel d'intégration approprié pendant l'installation du Gestionnaire de cellule.

La procédure d'installation dépend de l'environnement cluster où vous installez le client d'intégration. Consultez les sections à propos de la gestion des clusters correspondant à votre système d'exploitation :

- Installation de Data Protector sur Serviceguard, Page 166
- Installation de Data Protector sur Symantec Veritas Cluster Server, Page 177
- Installation de Data Protector sur Microsoft Cluster Server, Page 180
- Installation de Data Protector sur un cluster Microsoft Hyper-V, Page 192
- Installation de Data Protector sur un cluster IBM HACMP, Page 192

Pour plus d'informations sur la gestion des clusters, consultez l'index *Aide de Data Protector* : « cluster, Serviceguard » et le *Guide conceptuel Data Protector*.

Étapes suivantes

Une fois l'installation terminée, consultez le *Guide d'intégration Data Protector* pour avoir des informations sur la configuration de l'intégration.

Clients Microsoft Exchange Server

Les composants Data Protector qui doivent être installés sur les systèmes Microsoft Exchange Server dépendent de la solution de sauvegarde et de restauration que vous voulez utiliser. Vous pouvez choisir parmi les méthodes suivantes :

- Intégration Data Protector avec Microsoft Exchange Server 2007 , bas
- Intégration Data Protector avec Microsoft Exchange Server 2010 , Page 119
- Data Protector Intégration avec Microsoft Exchange Server Single Mailbox, Page 119
- Data Protector Intégration de Microsoft VSS (Volume Shadow Copy Service), Page 120
- Data Protector Extension de restauration granulaire pour Microsoft Exchange Server, Page 120

Intégration Data Protector avec Microsoft Exchange Server 2007

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

L'Agent d'intégration Microsoft Exchange Single Mailbox sera installé en tant que partie du composant d'intégration de Data Protector avec Microsoft Exchange Server.

Conditions préalables

- Microsoft Exchange Server doit être opérationnel.
- Vous devez connaître l'architecture de base de Microsoft Exchange Server. Pour plus d'informations sur Microsoft Exchange Server, consultez *l'aide en ligne de Microsoft Exchange Server*.
- Vous possédez une licence d'utilisation (LTU) d'extension pour sauvegarder Data Protector en ligne afin de pouvoir utiliser l'intégration de Data Protector avec Microsoft Exchange Server.
- Si vous comptez utiliser l'intégration avec Microsoft Exchange Server sur une baie de disques, installez les services Exchange Server - Banque d'informations, Service de gestion des clés (optionnel), le service de réplication de site (optionnel) - sur les volumes source de la baie de disques, sur le système d'application.

Procédure

1. Sur le système d'Exchange Server, ajoutez le répertoire *Exchange_Server_home*\bin au chemin du système.
   a. Sur le bureau Windows, cliquez avec le bouton droit sur **Poste de travail**, puis sur **Propriétés**.
   b. Dans la fenêtre Propriétés système, cliquez sur **Avancé**, puis sur **Variables d'environnement**.
   c. Dans la zone du groupe Variables système, dans la liste des variables, localisez l'entrée **Chemin** et cliquez sur **Modifier**.
   d. Dans la fenêtre Editer la variable système, dans la zone de texte Valeur de la variable, ajoutez le répertoire *Exchange_Server_home*\bin. Cliquez sur **OK**.

   > **IMPORTANT :**
   > Si Exchange Server est compatible cluster, ajoutez ce répertoire au chemin du système sur tous les nœuds du cluster.

2. Installez le logiciel d'intégration avec Microsoft Exchange Server sur votre système Exchange Server (client Data Protector) soit en local, depuis le package d'installation, soit à distance, en utilisant l'interface graphique de Data Protector.

   > **IMPORTANT :**
   > Si l'Exchange Server est compatible cluster, installez les composants logiciel en local, depuis le package d'installation, sur tous les nœuds du cluster.

   Si Data Protector est déjà installé sur le système Exchange Server ou si vous effectuez une installation à distance sur Exchange Server sans que Data Protector ne soit encore installé, utilisez l'interface graphique de Data Protector pour installer les composants logiciel requis.

   Si Data Protector n'est pas encore installé sur le système Exchange Server et que vous effectuez une installation en local, démarrez l'assistant de configuration de Data Protector. L'assistant de configuration vous guidera pendant le processus d'installation, qui est différent pour une installation d'un Gestionnaire de cellule de Data Protector et pour l'installation d'un client Data Protector.

   Il vous faut installer les composants logiciel Data Protector suivants :

   - Intégration avec MS Exchange
   - Agent de support général (si vous avez des périphériques connectés au système client d'Exchange Server)

   Il est également recommandé d'installer :

   - Interface utilisateur
   - Agent de disque (si vous effectuez une sauvegarde du système de fichier du système client d'Exchange Server pour tester)

3. Si l'Exchange Server est compatible cluster, assignez le compte de service du cluster au service Inet Data Protector sur tous les nœuds de cluster.

a. Sur le bureau Windows, cliquez avec le bouton droit sur **Poste de travail**, puis sur **Gérer**.
b. Dans la fenêtre Gestion de l'ordinateur, développez **Services et applications** et cliquez sur **Services**.
c. Dans la liste des services, localisez l'entrée **Data Protector Inet**, cliquez sur celle-ci avec le bouton droit de la souris, puis cliquez sur **Propriétés**. La fenêtre Propriétés de Data Protector Inet s'affiche.
d. Dans la page de propriétés Connexion, cliquez sur **Ce compte**.
e. Dans la zone de texte Ce compte, entrez le nom du compte du service Cluster. Vous pouvez éventuellement rechercher un nom en particulier en cliquant sur **Parcourir**.
f. Dans les zones de texte Mot de passe et Confirmer le mot de passe, entrez le mot de passe du compte.
g. Cliquez sur **OK**.
h. Dans le menu Fichier, cliquez sur **Quitter**.

Vérification de l'installation de l'intégration de Data Protector avec Microsoft Exchange Server

- Vérifiez si la variable d'environnement `Path` inclut également le répertoire *`Exchange_Server_home`*`\bin`.

  Si ce n'est pas le cas, ajoutez le chemin complet de ce répertoire à la variable `Path`.
- Vérifiez si le nom du Gestionnaire de cellule est correctement défini sur le système client Data Protector. Procédez comme suit :
  1. Recherchez la clé de registre suivante :

     `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Site`
  2. Vérifiez si le nom et les données de cette clé de registre sont respectivement `CellServer` et *`Cell_Manager_host_name`*. Si ce n'est pas le cas, réinstallez Data Protector sur ce client.

Vérification de Microsoft Exchange Server

- Vérifiez si les services Microsoft Exchange Server suivants fonctionnent :
  - Surveillance du système Microsoft Exchange (`MSExchangeSA`)
  - Microsoft Exchange Information Store (`MSExchangeIS`)

  Si ce n'est pas le cas, redémarrez Exchange Server.
- Sauvegardez et restaurez la banque d'informations Exchange Server à l'aide de l'utilitaire de sauvegarde Windows (Microsoft Windows Backup) au lieu de Data Protector. En cas d'échec, essayez d'identifier le problème en vérifiant l'installation et la configuration de Microsoft Exchange Server.

Intégration Data Protector avec Microsoft Exchange Server 2010

L'environnement Microsoft Exchange Server doit être opérationnel.

Pour pouvoir sauvegarder les bases de données de Microsoft Exchange Server 2010 ou 2013, installez les composants Data Protector suivants sur tous les systèmes Microsoft Exchange Server :

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

> **REMARQUE :**
> Pour les sessions de sauvegarde transportables VSS, 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 aussi être importé dans la cellule Data Protector. Pour savoir comment importer un client dans une cellule Data Protector, consultez l'index *Aide de Data Protector* : "importation, systèmes clients".

> **REMARQUE :**
> - L'intégration Data Protector Microsoft Exchange Server 2010 étant basée sur la technologie VSS, Data Protector installe automatiquement le composant `MS Volume Shadow Copy Integration` lorsque vous installez le composant `MS Exchange Server 2010+ Integration`. Si le composant `MS Volume Shadow Copy Integration` est déjà installé, il est mis à jour.
> - Lorsque vous supprimez le composant `MS Exchange Server 2010+ Integration` d'un système, le composant `MS Volume Shadow Copy Integration` n'est pas supprimé automatiquement. Notez également que vous ne pouvez pas supprimer le composant `MS Volume Shadow Copy Integration` d'un système où le composant `MS Exchange Server 2010+ Integration` est installé.

Data Protector Intégration avec Microsoft Exchange Server Single Mailbox

Microsoft Exchange Server doit être opérationnel.

Pour pouvoir sauvegarder les éléments de Microsoft Exchange Server Mailbox et du Dossier public, installez le composant `MS Exchange Integration` au système Microsoft Exchange Server. Dans un environnement DAG, installez le composant sur tous les systèmes Microsoft Exchange Server qui font partie d'un DAG.

Sur les systèmes Microsoft Exchange Server 2007, il vous faut installer un package supplémentaire pour activer la fonctionnalité de l'intégration de Data Protector avec Microsoft Exchange Single Mailbox. Le package s'appelle Microsoft Exchange Server MAPI Client and Collaboration Data Objects

(ExchangeMapiCdo.EXE), et peut être téléchargé gratuitement sur le site de Microsoft http://www.microsoft.com/downloads/Search.aspx?DisplayLang=en.

Data Protector Intégration de Microsoft VSS (Volume Shadow Copy Service)

Voir Clients de Microsoft Volume Shadow Copy Service, Page 127.

Data Protector Extension de restauration granulaire pour Microsoft Exchange Server

Utilisez l'extension Data Protector pour pouvoir récupérer des éléments individuels de la boîte aux lettres de Microsoft Exchange Server. Suivant la configuration de votre environnement Microsoft Exchange Server, installez le composant Data Protector correspondant sur :

- simple système Microsoft Exchange Server : il doit être installé sur ce système
- multiples systèmes Microsoft Exchange Server : il doit être installé sur chaque système Exchange Server sur lesquels le rôle Serveur de boîte aux lettres est configuré
- Dans un environnement de groupe de disponibilité de base de données (DAG) Microsoft Exchange Server : il doit être installé en DAG sur un des systèmes Exchange Server.

Conditions préalables

- Installez ce qui suit sur le système Microsoft Exchange Server choisi :
  - Le composant Data ProtectorMS Exchange Server 2010+ Integration
  - Le composant Data ProtectorUser Interface
  - Tous les composants non Data Protector requis
- Gardez le port TCP/IP 60000 (par défaut) disponible sur le système Microsoft Exchange Server choisi.

Client Microsoft Exchange Server

Installez ce qui suit :

- Microsoft Exchange Server

  Assurez-vous que l'environnement de Microsoft Exchange Server soit correctement installé et configuré.

  Pour connaître les versions, plateformes, périphériques pris en charge ou tout autre information, consultez les dernières matrices de prise en charge sur https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.

  Pour toute information quant à l'installation, la configuration et l'utilisation de Microsoft Exchange Server, consultez la documentation de Microsoft Exchange Server.
- Console de gestion Microsoft (MMC) 3.0 ou plus récent

- .NET Framework 3.5.1
- Services d'information internet (IIS) 6.0 ou plus récent

Data Protector Client

Installez les composants Data Protector suivants :

- Le composant Data Protector`User Interface`
- Le composant Data Protector`MS Exchange Server 2010+ Integration` sur tous les systèmes Microsoft Exchange Server

Assurez-vous d'avoir installé et configuré votre solution de sauvegarde de Data Protector comme décrit dans le *Guide d'installation Data Protector* et le *Guide d'intégration Data Protector*.

Autres services et logiciels non Data Protector

- Installez Windows PowerShell 1.0 ou plus récent (un package central de la structure de gestion de Windows)
- La seule localisation PowerShell prise en charge est l'anglais (l'OS Windows doit utiliser la localisation anglaise).
- Gardez le port TCP/IP 60000 (par défaut) disponible pour le service web de récupération granulaire.
- Configurez le pare-feu pour autoriser les nouveaux ports.

Environnements pris en charge

L'extension peut être intégrée avec Microsoft Exchange Server dans différents environnements Microsoft Exchange Server :

- un système indépendant Microsoft Exchange Server (environnement indépendant)
- plusieurs systèmes Microsoft Exchange Mailbox Server (systèmes à serveurs multiples)
- des environnements de groupes de disponibilité de base de données Microsoft Exchange Server (environnements DAG)

Suivant la configuration de votre environnement Microsoft Exchange Server, installez l'extension comme indiqué :

Environnement indépendant

Tous les services et toutes les données Microsoft Exchange Server sont installés sur un seul Microsoft Exchange Mailbox Server, ce qui est suffisant pour les environnements de petite taille. Installez le composant `MS Exchange Granular Recovery Extension` sur le système Exchange Mailbox Server.

Environnement de systèmes Exchange Server multiples

Votre environnement contient plus d'une base de données Microsoft Exchange Server. Installez le composant `MS Exchange Granular Recovery Extension` sur le système Exchange Mailbox Server dont vous voulez récupérer des éléments.

Environnement DAG

Votre environnement peut contenir jusqu'à 16 systèmes Microsoft Exchange Mailbox Server. Installez le composant `MS Exchange Granular Recovery Extension` sur un nœud système du rôle de la boîte aux lettres de Microsoft Exchange Server. Une fois le composant installé, l'interface graphique de l'extension de restauration granulaire affiche tous les objets de base de données de boîte aux lettres de

tous les nœuds de Mailbox Server dans l'environnement DAG. L'extension considère automatiquement le comportement dynamique de l'environnement DAG.

Environnement CCR

Installez le composant `MS Exchange 2010 Granular Recovery Extension` sur un nœud de serveur de boîte aux lettres.

Environnement LCR

Installez le composant `MS Exchange 2010 Granular Recovery Extension` sur le serveur où sont situées les bases de données des boîtes aux lettres passives et actives.

Pour plus d'informations sur les concepts de Microsoft Exchange Server, consultez la documentation de Microsoft Exchange Server.

Installer l'extension

L'Extension de restauration granulaire Data Protector pour Microsoft Exchange Server fournie en tant que composant Data Protector. Le composant `MS Exchange Granular Recovery Extension` contient l'interface graphique, les options de ligne de commande, les composants service web et l'aide contextuelle (F1) de l'Extension de restauration granulaire. Tout le contenu doit être installé ensemble.

> **REMARQUE :**
> L'extension doit être installée sur les systèmes rôle de la boîte aux lettres Microsoft Exchange Server uniquement dans l'organisation Microsoft Exchange. Ces systèmes contiennent la base de données de la boîte aux lettres Microsoft Exchange Server et la technologie de récupération telle que Recovery Databases (RDB) requis pour restaurer complètement des bases de données et des éléments de boîte aux lettres récupérés de Microsoft Exchange Server.

Procédure

Installez l'extension en utilisant l'interface graphique de Data Protector :

> **IMPORTANT :**
> Assurez-vous de posséder les privilèges administrateur du compte d'utilisateur local Windows SYSTEM ou d'un compte d'utilisateur de domaine Windows sur le système de rôle de la boîte aux lettres de Microsoft Exchange Server. Vous devez être autorisé à créer des entrées de registre et à installer des fichiers ou des dossiers dans le répertoire `Program Files`.

1. Lancez une installation à distance d'un client en :
   - ajoutant un client
   - important un client
2. Ajoutez le composant `MS Exchange Granular Recovery Extension` au système client Data Protector.

Pour plus d'informations au sujet de l'installation de Data Protector, consultez «Installer des systèmes client», «Importer des systèmes clients», et «ajouter des composants Data Protector» que vous pouvez retrouver dans le Guide d'installation Data Protector.

Supprimer l'extension

Sélectionnez l'une des méthodes suivantes :

- Utilisez l'interface graphique de Data Protector pour supprimer à distance le client qui a reçu l'installation de l'extension.

  Pour plus d'informations sur la suppression de clients Data Protector consultez l'index *Aide de Data Protector* : "désinstaller, client".
- Supprimez manuellement le composant `MS Exchange Granular Recovery Extension`.

  Pour plus d'informations sur la suppression des composants logiciels Data Protector, consultez l'index *Aide de Data Protector* : "désinstaller, logiciel Data Protector".

Clients Microsoft SQL Server

On suppose que votre Microsoft SQL Server est opérationnel.

Afin de pouvoir sauvegarder la base de données de Microsoft SQL Server, vous devez sélectionner le composant `MS SQL Integration` au cours de la procédure d'installation.

Clients Microsoft SharePoint Server

Les composants Data Protector devant être installés dans un environnement Microsoft SharePoint Server varient en fonction de la solution de sauvegarde et de restauration que vous voulez utiliser. Vous pouvez choisir parmi les méthodes suivantes :

- Data Protector Microsoft SharePoint Server 2007/2010/2013 integration, bas
- Data Protector Solution basée sur Microsoft SharePoint Server VSS, Page suivante
- Data Protector Intégration de Microsoft VSS (Volume Shadow Copy Service), Page suivante
- Data Protector Extension de restauration granulaire pour Microsoft SharePoint Server, Page suivante

Data Protector Microsoft SharePoint Server 2007/2010/2013 integration

On suppose que votre Serveur Microsoft SharePoint et le Microsoft SQL Server sont opérationnels.

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

- `MS SharePoint 2007/2010/2013 Integration` – sur les systèmes Microsoft SharePoint Server (les systèmes Microsoft SQL Server sont exclus)
- `MS SQL Integration` - sur les systèmes Microsoft SQL Server

> **REMARQUE :**
> Si un système dispose de Microsoft SQL Server et Microsoft SharePoint Server, installez les

deux composants Data Protector sur celui-ci.

Data Protector Solution basée sur Microsoft SharePoint Server VSS

On suppose que votre Serveur Microsoft SharePoint et le Microsoft SQL Server sont opérationnels.

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

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

  Microsoft Office SharePoint Server 2007 :

  - `Windows SharePoint Services Database`
  - `Windows SharePoint Services Help Search`
  - `Office SharePoint Server Search`

  Microsoft SharePoint Server 2010 :

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

  Microsoft SharePoint Server 2013 :

  - `SharePoint Foundation Database`
  - `SharePoint Server Search`

- Le composant Data Protector`User Interface` est l'un des systèmes Microsoft SharePoint Server avec le composant Data Protector`MS Volume Shadow Copy Integration` installé et sur lequel vous envisagez de configurer et de démarrer une sauvegarde.

Data Protector Intégration de Microsoft VSS (Volume Shadow Copy Service)

Voir Clients de Microsoft Volume Shadow Copy Service, Page 127.

Data Protector Extension de restauration granulaire pour Microsoft SharePoint Server

On suppose que votre Serveur Microsoft SharePoint et le Microsoft SQL Server sont opérationnels.

Afin de pouvoir récupérer des objets Microsoft SharePoint Server individuels, installez la `MS SharePoint Granular Recovery Extension` sur le système d'administration centrale de Microsoft SharePoint Server.

- Lors de l'installation locale du composant, l'assistant d'installation Data Protector affichera la boîte de dialogue Options de l'extension de restauration granulaire MS SharePoint. Indiquez le nom d'utilisateur de l'administrateur de la batterie et le mot de passe.
- Pour installer ce composant à distance, sélectionnez la `MS SharePoint Granular Recovery Extension`, cliquez sur **Configurer** et indiquez le nom d'utilisateur de l'administrateur de la batterie et le mot de passe dans la boîte de dialogue Options de l'extension de restauration granulaire MS SharePoint.

> **REMARQUE :**
> - Vous pouvez uniquement installer l'extension de restauration granulaire sur les systèmes équipés de Microsoft SharePoint Server.
> - Assurez-vous que les composants Data Protector nécessaires pour sauvegarder les données de Microsoft SharePoint Server sont également installés dans l'environnement de Microsoft SharePoint Server.

Conditions préalables

- **Packages Microsoft :**

  Installez ce package central d'architecture de gestion Windows :
  - Microsoft PowerShell 2.0 ou version ultérieure

- **Packages Microsoft SQL Server :**

  Installez les packages suivants pour Microsoft SQL Server 2005 ou Microsoft SQL Server 2008 :
  - Client natif de Microsoft SQL Server
  - Microsoft Core XML Services (MSXML) 6.0
  - Regroupement d'objets de gestion Microsoft SQL Server 2008

  Installez les packages suivants pour Microsoft SQL Server 2012 :
  - Client natif de Microsoft SQL Server
  - Microsoft Core XML Services (MSXML) 6.0 ou version ultérieure
  - Regroupement d'objets de gestion Microsoft SQL Server 2012

  Ces packages doivent être installés sur tous les systèmes Microsoft SharePoint Server sur lesquels au moins un des services suivants est activé :
  - Administration centrale
  - Application Web Windows SharePoint Services (Microsoft Office SharePoint Server 2007)
  - Application Web Microsoft SharePoint Foundation (Microsoft SharePoint Server 2010/2013)

Vous pouvez télécharger les packages à partir du site Web : http://www.microsoft.com/downloads/en/default.aspx.

Recherchez le **package de fonctions pour Microsoft SQL Server 2008** ou le **package de fonctions Microsoft SQL Server 2012**.

- **Data Protector composants :**

  Assurez-vous d'avoir installé et configuré votre solution de sauvegarde Data Protector décrite dans :

  - *Guide d'installation Data Protector*
  - chapitres applicables de *Guide d'intégration Data Protector*
  - *Guide d'intégration Data Protector Sauvegarde avec temps d'indisponibilité nul*
  - *Guide d'intégration Data Protector pour Microsoft VSS*

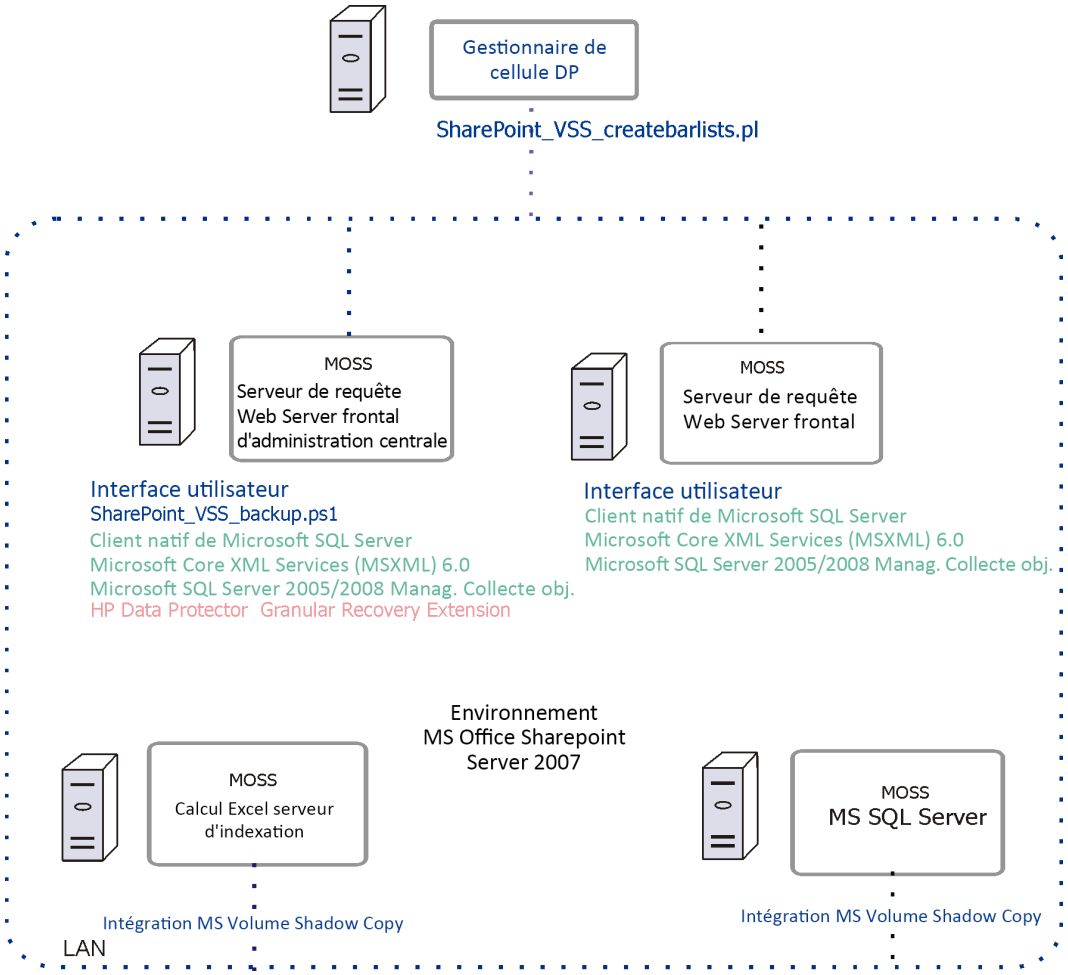
  Par ailleurs, assurez-vous que le composant Data Protector`User Interface` est installé sur tous les systèmes Microsoft SharePoint Server sur lesquels au moins un des services suivants est activé :

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

Environnement d'extension de restauration granulaire

Dans Installation d'une batterie de support qui utilise la solution basée sur Data Protector Microsoft SharePoint Server VSS (un exemple) , Page suivante, les composants Data Protector sont colorés en bleu, les packages d’installation de Microsoft SQL Server sont en vert, et le composant d'extension de récupération granulaire Data Protector est rouge.

Installation d'une batterie de support qui utilise la solution basée sur Data Protector Microsoft SharePoint Server VSS (un exemple)



Clients de Microsoft Volume Shadow Copy Service

Pour sauvegarder les modules d'écriture MS Volume Shadow Copy ou seulement le système de fichiers utilisant MS Volume Shadow Copy, installez les composants logiciels Data Protector suivants sur le système d'application (sauvegarde locale) ou sur le système d'application ET de sauvegarde (sauvegarde transportable) :

- `MS Volume Shadow Copy Integration`.
- Si vous utilisez une baie de disques (avec les fournisseurs matériels), l'agent de baie de disques approprié : `P4000 VSS Agent`, `P6000 / 3PAR SMI-S Agent`, `P9000 XP Agent` ou `3PAR VSS Agent`.

Après avoir installé l'intégration VSS, vous devez résoudre les volumes sources sur le système d'application si vous voulez effectuer les sessions ZDB sur disque et ZDB sur disque + bande (sessions de restauration instantanée activées). Exécutez l'opération de résolution à partir d'un client VSS dans la cellule comme suit :

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

Cependant, si vous ne pouvez résoudre ou si vous échouez à résoudre le système d'application, il sera résolu automatiquement, tant que l'option `OB2VSS_DISABLE_AUTO_RESOLVE` dans le fichier `omnirc` est définie sur `0` (par défaut). Dans ce cas, la durée de sauvegarde pour la création d'une réplique est prolongée.

Pour plus d'informations, reportez-vous à *Guide d'intégration Data Protector Sauvegarde avec temps d'indisponibilité nul*.

Clients Sybase Server

On suppose que votre serveur de sauvegarde Sybase est opérationnel.

Pour sauvegarder la base de données Sybase, vous devez sélectionner le composant Data Protector suivant au cours de la procédure d'installation :

- `Sybase Integration` - pour permettre la sauvegarde d'une base de données Sybase
- `Disk Agent` - installez l'agent de disque pour deux raisons :
  - Pour exécuter une sauvegarde du système de fichiers du serveur de sauvegarde Sybase. Effectuez cette sauvegarde *avant* de configurer votre intégration Data Protector Sybase et vous pouvez résoudre tous les problèmes associés au serveur de sauvegarde Sybase et Data Protector.
  - Pour exécuter une sauvegarde du système de fichiers des données importantes qui ne *peuvent pas* être sauvegardées à l'aide du serveur de sauvegarde Sybase.

Clients Informix Server

On suppose que votre Informix Server est opérationnel.

Pour sauvegarder la base de données Informix Server, vous devez sélectionner le composant Data Protectorsuivant au cours de la procédure d'installation :

- `Informix Integration` - pour permettre la sauvegarde d'une base de données Informix Server
- `Disk Agent` - installez l'agent de disque pour deux raisons :
  - Pour exécuter une sauvegarde du système de fichiers de Informix Server. Effectuez cette sauvegarde *avant* de configurer votre intégration Data Protector Informix Server et vous pouvez résoudre tous les problèmes associés à Informix Server et Data Protector.
  - Pour exécuter une sauvegarde du système de fichiers des données importantes de Informix Server (notamment, le fichier ONCONFIG, le fichier `sqlhosts`, le fichier d'amorçage d'urgence ON-Bar, `oncfg_`*`INFORMIXSERVER`*`.`*`SERVERNUM`*, les fichiers de configuration, et ainsi de suite) qui *ne peuvent pas* être sauvegardées à l'aide de ON-Bar.

IBM HACMP Cluster

Si Informix Server est installé dans l'environnement IBM HACMP Cluster, installez le composant `Informix Integration` sur tous les nœuds du cluster.

Clients SAP R/3

Conditions préalables

- Assurez-vous que le logiciel Oracle suivant est installé et configuré :
  - Oracle Enterprise Server (RDBMS)
  - Logiciel Oracle Net8
  - SQL*Plus
- On suppose que votre serveur de base de données SAP R/3 est opérationnel.

> **REMARQUE :**
> Les spécifications de sauvegarde de l'intégration Data Protector SAP R/3 sont complètement compatibles avec la version précédente de Data Protector. Data Protector exécutera toutes les spécifications de sauvegarde créées par les versions antérieures de Data Protector. Vous ne pouvez pas utiliser les spécifications de sauvegarde créées par la version actuelle de Data Protector sur les versions antérieures de Data Protector.

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

- `SAP R/3 Integration`
- `Disk Agent`

  Data Protector requiert l'installation d'un agent de disque sur les serveurs de sauvegarde (clients avec les données du système de fichiers à sauvegarder).

Clients SAP MaxDB

On suppose que votre serveur SAP MaxDB est opérationnel.

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

- `SAP MaxDB Integration` - afin d'exécuter une sauvegarde en ligne intégrée d'une base de données de SAP MaxDB
- `Disk Agent` - afin d'exécuter une sauvegarde de système de fichiers d'une base de données de SAP MaxDB.

Clients SAP HANA Appliance

Pour intégrer Data Protector à votre appareil SAP HANA (SAP HANA), installez les composants logiciels Data Protector suivants sur le système SAP HANA :

- SAP HANA Integration

  Ce composant active la sauvegarde intégrée d'une base de données SAP HANA complète et les journaux de rétablissement SAP HANA.

- Disk Agent

  Ce composant active la sauvegarde non intégrée des fichiers de configuration SAP HANA à l'aide de la fonctionnalité de sauvegarde de système de fichiers Data Protector. Après un sinistre, si vous disposez d'une image de sauvegarde des fichiers de configuration SAP HANA, cela peut vous aider à identifier et à restaurer plus facilement vos modifications.

Dans le cas d'un environnement SAP HANA partagé, installez les composants ci-dessus sur chaque système SAP HANA qui constitue un tel environnement.

Clients Oracle Server

On suppose que votre serveur Oracle est opérationnel.

Afin de pouvoir sauvegarder la base de données Oracle, vous devez sélectionner le composant Oracle Integration au cours de la procédure d'installation.

HP OpenVMS

Sur HP OpenVMS, après avoir installé l'intégration Oracle et l'avoir configurée comme indiqué dans *Guide d'intégration Data Protector*, vérifiez que l'entrée -key Oracle8 est présente dans OMNI$ROOT:[CONFIG.CLIENT]omni_info, par exemple :

```
-key oracle8 -desc “Oracle Integration” -nlsset 159 -nlsId 12172 -flags 0x7 -ntpath ““ -uxpath ““ -version 9.08
```

Si l'entrée n'est pas présente, copiez-la à partir de OMNI$ROOT:[CONFIG.CLIENT]omni_format. Dans le cas contraire, l'intégration Oracle n'apparaîtra pas comme étant installée sur le client OpenVMS.

Clients MySQL

Pour intégrer la protection de données dans votre système de gestion de base de données MySQL, et pour pouvoir sauvegarder les instances et les données MySQL, installez les éléments suivants Data Protector sur l’hôte MySQL :

- MySQL Integration

  Cet élément permet une sauvegarde intégrée et une restauration des bases de données MySQL

- Disk Agent

  Cet élément permet de sauvegarder les évènements binaires et de restaurer les évènements binaires comme prérequis pour la restauration de la base de données MySQL. Il peut aussi s’utiliser pour une sauvegarde non-intégrée des données MySQL en vue de résoudre des problèmes avec le Data Protector du client où MySQL est installé.

Clients PostgreSQL

Pour intégrer Data Protector à votre système de serveur de base de données PostgreSQL et pour pouvoir sauvegarder les données et instances PostgreSQL, installez les composants Data Protectorsuivants sur l'hôte PostgreSQL :

- `PostgreSQL Integration`

  Ce composant permet une sauvegarde et une restauration intégrées des bases de données PostgreSQL.

Clients IBM DB2 UDB

On suppose que votre serveur DB2 est opérationnel.

Afin de pouvoir sauvegarder la base de données DB2, vous devez sélectionner les composants `DB2 Integration` et `Disk Agent` au cours de la procédure d'installation.

Dans un environnement physiquement partitionné, installez les composants `DB2 Integration` et `Disk Agent` sur chaque nœud physique (système) sur lequel se trouve la base de données.

> **REMARQUE :**
> Connectez-vous en tant qu'utilisateur `root` pour effectuer l'installation.

Clients Lotus Notes/Domino Server

On suppose que votre serveur Lotus Notes/Domino est opérationnel.

Afin de pouvoir sauvegarder la base de données du serveur Lotus Notes/Domino, vous devez sélectionner les composants `Lotus Integration` et le `Disk Agent` au cours de la procédure d'installation. Vous devrez disposer du composant `Disk Agent` pour pouvoir sauvegarder les données du système de fichiers avec Data Protector à des fins suivantes :

- La sauvegarde des données importantes *ne peut pas* être effectuée à l'aide de l'agent Intégration Lotus. C'est ce que l'on appelle les fichiers hors base de données, qui doivent être sauvegardés pour fournir une solution complète de protection des données pour un serveur Lotus Notes/Domino, tels que `notes.ini`, `desktop.dsk`, tous les `*.id files`.
- Test de la sauvegarde du système de fichiers pour résoudre les problèmes de communication et les autres problèmes liés à l'application et Data Protector.

Cluster Lotus Domino

Installez les composants L`Lotus Integration` et le `Disk Agent`sur les serveurs Domino qui seront utilisés pour la sauvegarde et, si vous prévoyez de restaurer les bases de données Domino sur d'autres serveurs Domino contenant des répliques de ces bases de données, installez également ces composants sur ces serveurs Domino.

Clients VMware

Les composants Data Protector qui doivent être installés sur les systèmes VMware varient en fonction de la solution de restauration et de récupération que vous souhaitez utiliser.

Cette section du guide vous aide avec :

- Environnement GRE
- Installation de Data Protector GRE
- Désinstallation de Data Protector GRE

Data Protector GRE for VMware vSphere

L'extension de restauration granulaire Data Protector permet de restaurer les données à l'aide de l'intégration de l'environnement virtuel Data Protector. Cette extension est uniquement une solution de récupération. L'environnement d'extension de restauration granulaire (GRE), y compris le Mount Proxy et vCenter Server, ont des exigences spécifiques à satisfaire avant de pouvoir installer les modules GRE.

Le plug-in GRE est accessible depuis l'interface utilisateur du module d'extension Advanced GRE Web Plug-in.

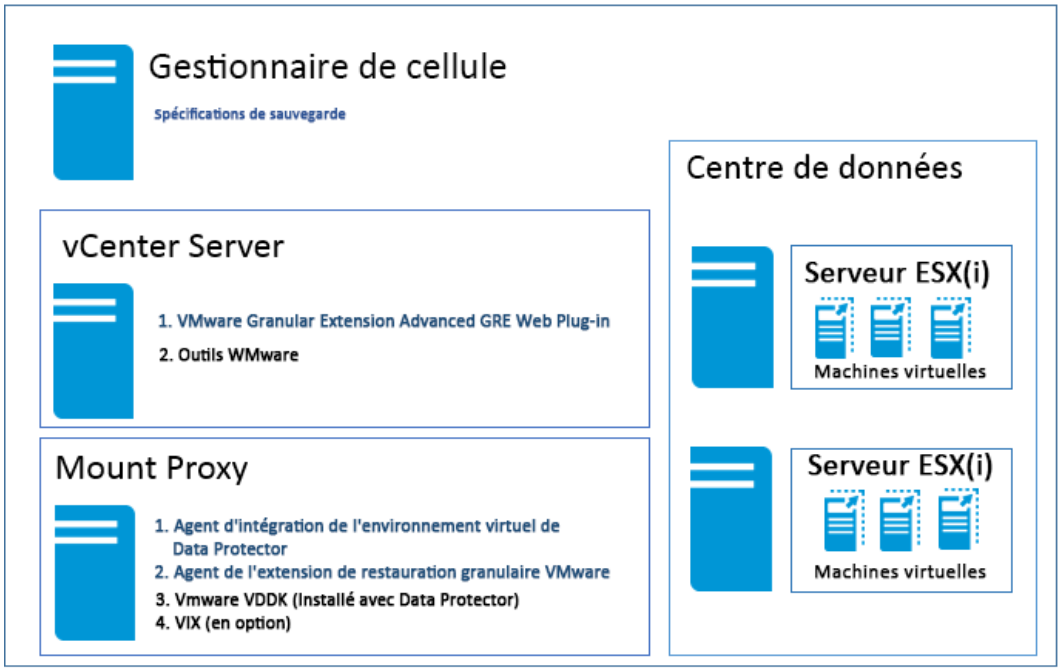
Cette section du guide fournit les informations nécessaires permettant de créer cet environnement.

Environnement GRE

Dans l'illustration suivante

- Les composants Data Protector sont indiqués en bleu.
- Les composants VMware sont indiqués en noir.

Installation de Data Protector l'extension de restauration granulaire



Système Mount Proxy

L'extension de restauration granulaire Data Protector pour VMware vSphere requiert un système Mount Proxy comme emplacement temporaire de restauration ou de récupération entre l'emplacement d'origine et l'emplacement cible sur le système de serveur VMware vCenter. Tout système pris en charge, également une machine virtuelle, peut être utilisé comme système Mount Proxy.

Les disques de la machine virtuelle ne sont pas montés immédiatement. La session de montage commence lorsque, en tant qu'utilisateur VMware vCenter, vous commencez à parcourir les fichiers en utilisant l'extension intégrée dans l'environnement vCenter.

Votre système Mount Proxy doit disposer de suffisamment d’espace disque pour accueillir les données restaurées. Vous pouvez également ajuster l'espace disque à la demande en connectant des disques supplémentaires ou en ajoutant un autre système Mount Proxy.

> **REMARQUE :**
> il est recommandé de configurer un système dédié comme système de proxy de montage.

Configuration requise du système

Les conditions requises du système suivant doivent répondre au système de proxy de montage :

- **Systèmes Windows :**
  (Facultatif) Veillez à installer l'utilitaire suivant, si vous souhaitez utiliser VIX API pour la récupération des fichiers : VX est utilisé comme option de repli lorsque le partage de réseau n'est pas disponible.
  - VMware VIX API 1.14
- **Systèmes Linux :**
  Assurez-vous d'installer les composants et outils du système d'exploitation suivants :

- FUSE 2.7.3 ou version ultérieure.*
- Package cifs-utils (utilisé pour le montage des disques de la machine virtuelle Windows sur un système de proxy de montage Linux)
- Package ntfs-3g (utilisé pour le montage des disques de la machine virtuelle Windows sur un système de proxy de montage Linux)
- services NFS
- VMware VIX API 1.14 (facultatif ; utilisé pour la récupération de fichiers et comme une option de reprise lorsque le partage réseau n'est pas disponible)
- kpartx est nécessaire pour les disques avec des partitions LVM
- Serveur Samba, comme Data Protector utilise le serveur Samba pour créer les partages au cours de la récupération. Vérifiez que les partages Samba disposent des autorisations en lecture-écriture. Si le module de sécurité Security-Enhanced Linux (SELinux) du noyau est déployé sur votre système Linux, exécutez la commande `# setsebool -P samba_export_all_rw on` pour activer les autorisations en lecture/écriture au niveau des partages Samba.
- Ajoutez l'utilisateur de l'hôte Media Agent à la base de données de mots de passe samba à l'aide de la commande suivante : `smbpasswd –a <user>`. Vous pouvez vérifier si l'utilisateur a été ajouté à la base de données de mots de passe à l'aide de la commande suivante :`pdbedit -w -L`
- Le pare-feu Windows doit être configuré. Pour plus d'informations sur la configuration, reportez-vous à la section "Configuration des exceptions du pare-feu Windows" dans le *Guide de l'utilisateur Data Protector Granular Recovery Extension.*

> **REMARQUE :**
> 1. Pour des informations détaillées sur la configuration des périphériques Smart Cache, reportez-vous à la section " Configurer Smart Cache" dans le *Data ProtectorGuide de l'administrateur*.
> 2. Pour plus d'informations sur la configuration des périphériques StoreOnce, consultez la section « Configuration d'une sauvegarde sur un périphérique de disque – StoreOnce » dans le *Data ProtectorGuide de l'administrateur*.

*pour SUSE Linux Enterprise Server (SLES) - utilisez FUSE 2.7.2

*Pour SUSE Linux Enterprise Server 12 (SLES 12) - use FUSE 2.9.3

Composants Data Protector requis sur le système de proxy de montage

Installez le client Data Protector. Installez à distance les composants Data Protector suivants sur le système de proxy de montage :

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

Consultez l'écran Sélection des composants. Vous devez sélectionner ce composant au cours de la procédure d'installation. Voir Installer des clients Data Protector, Page 54.

En cas d'échec de l'installation à distance, installez l'extension sur votre système local. Consultez la section "Solution d'installation locale" dans *Guide de l'utilisateur Data Protector Granular Recovery Extension.* Cependant, pour les mises à jour de correctifs, vous devez installer l'agent GRE à distance.

Pour plus d'informations sur la procédure d'importation, consultez la section "Configuration de l'intégration" dans *Guide d'intégration Data Protector*.

Les périphériques à boucle Linux ne sont pas créés par défaut pour RHEL 7.0 et SLES 12. Assurez-vous qu'il existe suffisamment de périphériques Linux en boucle sur le système de proxy de montage. Vous devez avoir autant de périphériques en boucle que de disques montés afin que le groupe de volume logique complet soit disponible.

> **REMARQUE :**
> Redémarrez votre système avant d'installer `VMware Granular Recovery Extension Agent`, si vous avez ajouté ou supprimé l'un quelconque des composants Data Protector ou des VDDK VMware.

> **REMARQUE :**
> Lors de l’installation du composant `VMware Granular Recovery Extension Agent` sur le système Mount Proxy, il arrive que l’utilisateur soit être averti dans la sortie de la session d’installation qu'un redémarrage de l’hôte cible doit être effectué pour terminer l’installation.

> **REMARQUE :**
> Le client que vous essayez d'utiliser comme hôte de sauvegarde *ne doit pas* disposer du logiciel de sauvegarde consolidée VMware (VCB) installé.

Serveur VMware vCenter (serveur VirtualCenter)

L'extension de restauration granulaire Data Protector (GRE) de VMware vSphere est intégrée au serveur VMware vCenter. Vous accédez aux machines virtuelles à l'aide du client Web VMware vSphere. L'onglet Data Protector est ajouté à l'interface du client Web VMware vSphere.

> **REMARQUE :**
> Le module d'extension Advanced GRE Web Plug-in pour GRE est pris en charge par le client Web VMware vSphere à partir de la version 5.5.0 U2.

Environnement VMware vCenter Server Appliance (VCSA) 6.0

Conditions préalables

Vous devez exécuter les commandes suivantes sur le serveur VCSA :

```
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -F
```

Installation de Data Protector GRE pour VMware vSphere Web Client

Points à prendre en considération

1. Les machines virtuelles sur lesquelles vous envisagez d'effectuer les opérations de récupération doivent disposer des outils VMware 4.x ou versions ultérieures. Vous pouvez télécharger le package d'installation outils VMware sur la page http://www.vmware.com/download.
2. Seule l'installation à distance du client Web Data Protector Granular Recovery Extension pour VMware vSphere est prise en charge.
3. Afin de garantir la fonctionnalité adéquate de l'extension, n'installez et ne configurez pas ensemble le système de serveur VMware vCenter et un système de proxy de montage sur le même système client.
4. Assurez-vous que les versions des composants `VMware Granular Recovery Extension Agent`, `Virtual Environment Integration Agent` et Data Protector Gestionnaire de cellule sont identiques. Les versions d'agent mixtes ne sont pas prises en charge.

Conditions préalables

Pour utiliser l'extension, vous devez installer et configurer les systèmes suivants :

- Cellule et client **Data Protector**
- Système de serveur VMware vCenter
- Système Mount Proxy

Le plug-in GRE est accessible depuis l'interface utilisateur du module d'extension Advanced GRE Web Plug-in.

Nouvelle installation

Accomplissez les étapes suivantes pour installer GRE pour le client Web VMware vSphere.

Environnement : Data Protector nouvelle version (9.02 ou supérieure), vCenter (voir la matrice de prise en charge de la virtualisation pour connaître les versions compatibles), et module d'extension Web GRE avancé.

Étape 1 : configurez l'instance Gestionnaire de cellule.

Le Gestionnaire de cellule peut être installé sur le système Windows et Linux.

Étape 2 : configurez l'instance Serveur d'installation.

Le serveur d'installation est ajouté par défaut dans le cadre de l'installation de Gestionnaire de cellule installation.

- Si vous avez installé le serveur d'installation Windows avec Gestionnaire de cellule sur Windows (option par défaut), vous pouvez ignorer cette étape et passer à la configuration de Mount Proxy.

- Si le Gestionnaire de cellule est installé sur Linux, vous devez alors configurer un serveur d'installation Windows et l'importer vers le Gestionnaire de cellule sur Linux.

Étape 3 : configurez les systèmes Mount Proxy.

- Peut être réalisée sur un système Windows et/ou Linux.
- Il est recommandé d'avoir le Mount Proxy sur une machine différente et dédiée autre que le Gestionnaire de cellule.
- Le client Data Protector doit être installé sur la machine Mount Proxy avec les composants suivants installés :
  1. `Virtual Environment Integration`
  2. `VMware Granular Recovery Extension Agent`.

Étape 4 : configurez le serveur vCenter.

- Le vCenter peut se trouver dans un environnement Windows ou Linux.
- Le client Data Protector n'est pas requis.

Étape 5 : installez le module d'extension Web GRE avancé sur le serveur vCenter.

1. Pour importer la machine vCenter en tant que client vCenter vers le Data Protector Gestionnaire de cellule.
   a. Cliquez sur **Clients** avec le bouton droit de la souris, puis sélectionnez **Importer client**.
   b. Saisissez le nom d'hôte du vCenter et sélectionnez le type pour **VMware vCenter**. Cliquez sur **Suivant**.
   c. Entrez les informations d'identification du vCenter (les mêmes informations utilisées pour se connecter au client Web vCenter). Cochez la case **Module d'extension Web GRE avancé** et cliquez sur **Terminer**.

> **REMARQUE :**
> Vous pouvez inscrire et désinscrire le module d'extension Web GRE avancé respectivement à l'aide des commandes `omnicc -import_vcenter` et `omnicc -export_host` . Pour plus d'informations, reportez-vous au guide *Guide de référence de l'interface de ligne de commande Data Protector*.

> **REMARQUE :**
> Vous pouvez importer plusieurs instances de vCenter dans une entité Data Protector Gestionnaire de cellule.

Mise à niveau

Identifiez l’environnement applicable ou adapté à votre cas et exécutez les étapes de mise à niveau en consultant les rubriques suivantes :

Data Protector		**Modules d'extension**		
De	**A**	**Mise a jour depuis**	**A**	**Voir .**
Toutes les versions antérieures	DP 9.02 ou version ultérieure	Module Web	Module d'extension Advanced GRE	Option 1

			Web Plug-in	
DP 9.02 ou version ultérieure	Dernière version	Module d'extension Advanced GRE Web Plug-in	Module d'extension Advanced GRE Web Plug-in	Option 2

Option 1

Environnement : si vous effectuez une mise à niveau à partir d'une version antérieure de Data Protector avec le module d'extension Web vers une nouvelle version de Data Protector (9.02 ou version supérieure) avec le module d'extension Web GRE avancé, sur une instance vCenter 5.5 U2 ou version supérieure (voir la matrice de prise en charge de la virtualisation pour connaître les versions compatibles).

Si la procédure de mise à niveau de Data Protector upgrade est terminée, passez directement à l'étape 2.

Procédez comme suit :

1. Utilisez les programmes d'installations natifs de Data Protector (à la version requise) pour mettre à niveau l'instance Data Protector Gestionnaire de cellule
2. Faites un clic droit sur le client **vCenter** dans le Gestionnaire de cellule, puis cliquez sur **mettre à niveau**. (Comme l'utilisateur a configuré le module Web, la machine vCenter doit déjà être importée en tant que client Data Protector). Cette étape supprime le module d'extension Web existant du serveur vCenter et met à niveau le client Data Protectorsur vCenter vers la version requise.

   > **REMARQUE :**
   > Les fichiers de demande existants seront supprimés et vous devrez créer de nouvelles demandes.

3. Faites un clic droit sur le client dans le Gestionnaire de cellule, puis cliquez sur **mettre à niveau**. Répétez cette étape pour tous les proxy de montage et les autres clients.

   Pour importer la machine vCenter en tant que client vCenter vers le Data Protector Gestionnaire de cellule.

   a. Cliquez sur **Clients** avec le bouton droit de la souris, puis sélectionnez **Importer client**.
   b. Saisissez le nom d'hôte du vCenter et sélectionnez le type pour **VMware vCenter**. Cliquez sur **Suivant**.
   c. Entrez les informations d'identification du vCenter (les mêmes informations utilisées pour se connecter au client Web vCenter). Cochez la case **Module d'extension Web GRE avancé** et cliquez sur **Terminer**.

> **REMARQUE :**
> si nécessaire, le client Data Protector peut être conservé sur ce serveur vCenter.

Option 2

Environnement : si vous utilisez Data Protector 9.02 ou version supérieure avec le module d'extension Data Protector GRE avancé, pour obtenir les fonctionnalités mises à jour du module Web

GRE avancé avec la plus récente mise à niveau, procédez comme suit :

1. Pour désinscrire le module d'extension Web GRE avancé de Data Protector, ne cochez pas la case **Module d'extension Web GRE avancé** et cliquez sur **Appliquer**. Assurez-vous de supprimer toutes les instances de Gestionnaire de cellule la liste des hôtes du module d'extension Web GRE avancé.
2. Pour inscrire le module d'extension Web GRE avancé, cochez la case **Module d'extension Web GRE avancé** et cliquez sur **Appliquer**.

> **REMARQUE :**
> Assurez-vous que le Gestionnaire de cellule et tous les serveurs proxy sont mis à niveau.

Désinstaller le module d'extension Advanced GRE Web Plug-in

Si vous rencontrez des problèmes lors du lancement du module d'extension, accomplissez les étapes suivantes et redémarrez la procédure de mise à niveau prévue plus tôt, selon votre environnement.

Pour désinstaller le module d'extension Web GRE avancé

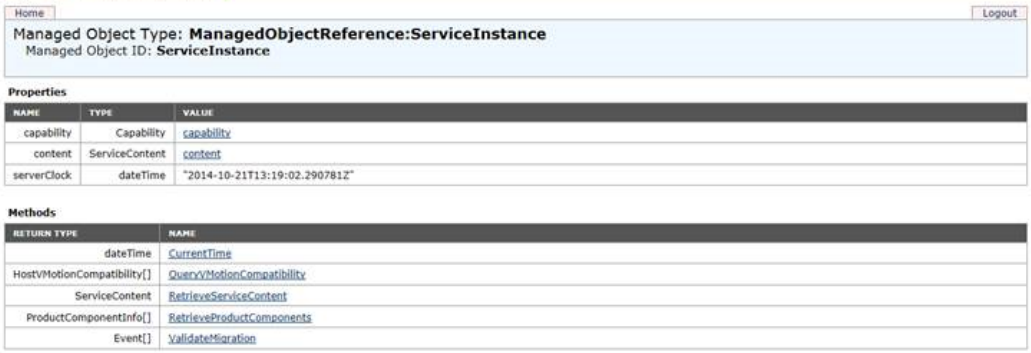
Pour désinstaller le module d'extension Web GRE avancé, ne cochez pas la case **Module d'extension Web GRE avancé** sous l'onglet Connexion du client VMware vCenter et cliquez sur **Appliquer**.

> **REMARQUE :**
> Si vous avez désinstallé une instance de Gestionnaire de cellule ou plusieurs instances de Gestionnaire de cellule sans désinscrire le module d'extension Web GRE avancé, vous verrez s'afficher l'onglet "Data Protector" sur le client Web VMware vSphere, mais vous ne pourrez pas vous y connecter. Vous devez désinscrire manuellement le plug-in Web GRE avancé. Pour plus de détails, reportez-vous à Désinscription manuelle de VMware vSphere Managed Object Reference

Désinscription manuelle de la référence à l'objet géré VMware vSphere

Suivez cette procédure pour supprimer un ou plusieurs gestionnaires de cellule enregistrés dans le vCenter.

1. Accédez à l'adresse URL de la référence à l'objet géré VMware vSphere : https://<vcenter>/mob


Home Logout

Managed Object Type: **ManagedObjectReference:ServiceInstance**
Managed Object ID: **ServiceInstance**

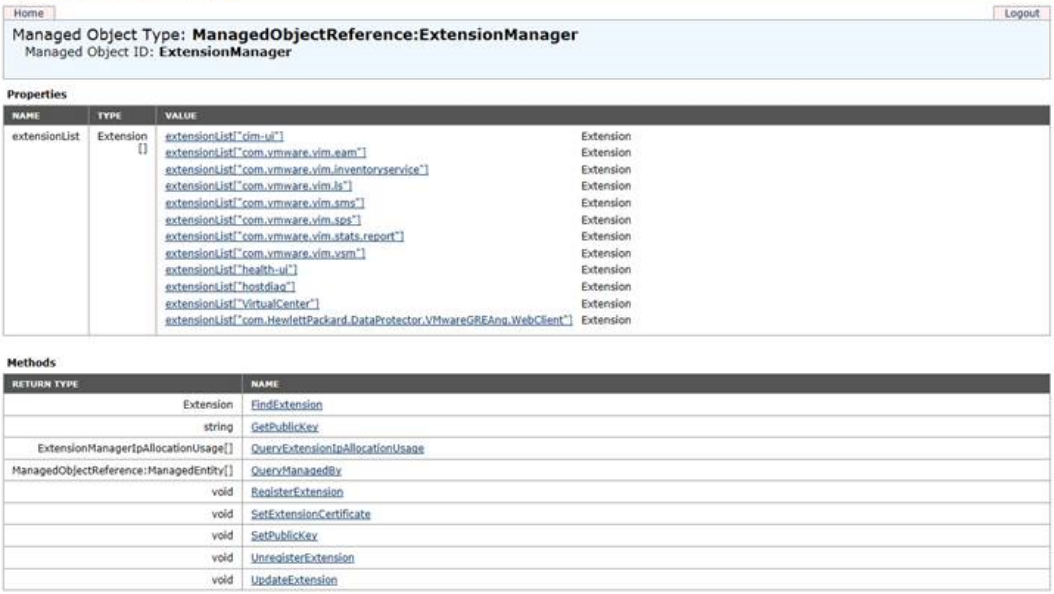
Properties

NAME	TYPE	VALUE
capability	Capability	capability
content	ServiceContent	content
serverClock	dateTime	"2014-10-21T13:19:02.290781Z"

Methods

RETURN TYPE	NAME
dateTime	CurrentTime
HostVMotionCompatibility[]	QueryVMotionCompatibility
ServiceContent	RetrieveServiceContent
ProductComponentInfo[]	RetrieveProductComponents
Event[]	ValidateMigration

2. Cliquez sur **Contenu** puis cliquez sur **ExtensionManager**.
3. Sélectionnez la clé com.HewlettPackardEnterprise.DataProtector.VMwareGREAng.WebClient


Home Logout

Managed Object Type: **ManagedObjectReference:ExtensionManager**
Managed Object ID: **ExtensionManager**

Properties

NAME	TYPE	VALUE	
extensionList	Extension[]	extensionList["cim-ui"]	Extension
		extensionList["com.vmware.vim.eam"]	Extension
		extensionList["com.vmware.vim.inventoryservice"]	Extension
		extensionList["com.vmware.vim.ls"]	Extension
		extensionList["com.vmware.vim.sms"]	Extension
		extensionList["com.vmware.vim.sps"]	Extension
		extensionList["com.vmware.vim.stats.report"]	Extension
		extensionList["com.vmware.vim.vsm"]	Extension
		extensionList["health-ui"]	Extension
		extensionList["hostdiag"]	Extension
		extensionList["VirtualCenter"]	Extension
		extensionList["com.HewlettPackard.DataProtector.VMwareGREAng.WebClient"]	Extension

Methods

RETURN TYPE	NAME
Extension	FindExtension
string	GetPublicKey
ExtensionManagerIpAllocationUsage[]	QueryExtensionIpAllocationUsage
ManagedObjectReference:ManagedEntity[]	QueryManagedBy
void	RegisterExtension
void	SetExtensionCertificate
void	SetPublicKey
void	UnregisterExtension
void	UpdateExtension

4. Cliquez sur **UnregisterExtension**, au bas de la page.

Clients Microsoft Hyper-V

Les composants Data Protector qui doivent être installés sur les systèmes Microsoft Hyper-V varient en fonction de la solution de sauvegarde et de restauration que vous souhaitez utiliser. Vous pouvez choisir parmi les méthodes suivantes :

- Clients Microsoft Hyper-V, haut
- Data Protector Intégration de Microsoft VSS (Volume Shadow Copy Service), Page suivante

Data Protector Intégration de l'environnement virtuel

On suppose que tous les systèmes sur lesquels vous essayez d'installer les composants sont opérationnels.

Sur les systèmes qui doivent contrôler la sauvegarde et les sessions de restauration (**hôtes de sauvegarde**), installez les composants Data Protector suivants :

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

> **REMARQUE :**
> Le composant `Disk Agent` vous permet d'utiliser le bouton **Parcourir** lors de la restauration vers un répertoire sur l'hôte de sauvegarde. Si le composant n'est pas installé, vous devez tapez le répertoire cible vous-même.

Sur les systèmes Microsoft Hyper-V, installez le composant Data Protector suivant :

- `MS Volume Shadow Copy Integration`

> **REMARQUE :**
> Si vos systèmes Microsoft Hyper-V sont configurés dans un cluster, ils doivent être installés en tant que clients compatibles cluster. Pour plus d'informations, voir Installation de Data Protector sur un cluster Microsoft Hyper-V, Page 192.

Sur les systèmes de sauvegarde (applicables aux sauvegardes VSS transportables), installez le composant Data Protector suivant :

- `MS Volume Shadow Copy Integration`

> **REMARQUE :**
> Un *hôte de sauvegarde* et un *système de sauvegarde* ne sont pas la même chose.

Data Protector Intégration de Microsoft VSS (Volume Shadow Copy Service)

Pour plus d'informations sur les composants devant être installés sur les systèmes Microsoft Hyper-V, consultez Clients Microsoft Hyper-V, Page précédente.

Clients NDMP Server

On suppose que votre serveur NDMP est opérationnel.

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

> **REMARQUE :**
> Si un client Data Protector n'est pas utilisé pour accéder à un lecteur dédié NDMP par le biais du serveur NDMP, mais qu'il est utilisé uniquement pour contrôler le robot de bibliothèque, soit le `NDMP Media Agent` soit le `General Media Agent` peut être installé sur un tel client.

Remarque : un seul agent de support peut être installé sur un client Data Protector.

Solutions P4000 SAN clients

Pour intégrer Solutions P4000 SAN avec Data Protector, installez les composants logiciels Data Protector suivants sur l'application et les systèmes de sauvegarde :

- `MS Volume Shadow Copy Integration`
- `P4000 VSS Agent`

Pour effectuer des sessions ZDB sur disque + bande ou ZDB sur bande, installez en plus le composant logiciel Data Protector suivant sur le système de sauvegarde :

- `General Media Agent`

Famille de baies de disques P6000 EVA clients

Pour intégrer Famille de baies de disques P6000 EVA avec Data Protector, installez les composants logiciels Data Protector suivants sur l'application et les systèmes de sauvegarde :

- `P6000 / 3PAR SMI-S Agent`
- `General Media Agent`

  Installez le composant `General Media Agent` sur le système de sauvegarde afin de sauvegarder les données de masse. Installez-le sur le système d'application afin de sauvegarder les journaux d'archive ou d'effectuer une restauration sur le système d'application.
- `Disk Agent`

  Installez le composant `Disk Agent` sur l'application et les systèmes de sauvegarde afin d'exécuter la sauvegarde avec temps d'indisponibilité nul des systèmes de fichiers ou images de disques. Les clients ne disposant pas de l'agent de disque ne sont pas répertoriés dans les listes déroulantes `Application system` et `Backup system` pendant la création d'une spécification de sauvegarde ZDB.

> **IMPORTANT :**
> Sur les systèmes Microsoft Windows Server 2008, deux correctifs Windows Server 2008 doivent être installés afin d'activer le fonctionnement normal de l'intégration Data Protector Famille de baies de disques P6000 EVA. Vous pouvez télécharger les packages de correctifs nécessaires sur les sites Web de Microsoft http://support.microsoft.com/kb/952790 et http://support.microsoft.com/kb/971254.
>
> Cette condition supplémentaire ne s'applique pas aux systèmes Windows Server 2008 R2.

Installation dans un cluster

Vous pouvez installer l'intégration Famille de baies de disques P6000 EVA dans un environnement de cluster. Pour connaître les configurations de cluster prises en charge et les conditions spécifiques d'installation, consultez le *Guide de l'administrateur Data Protector Sauvegarde avec temps d'indisponibilité nul*.

Intégration avec d'autres applications

Pour installer l'intégration Famille de baies de disques P6000 EVA avec une application de base de données, installez le composant Data Protector spécifique à l'intégration particulière sur l'application et les systèmes de sauvegarde, et effectuez les tâches d'installation spécifiques à cette intégration. Vous pouvez installer l'intégration Famille de baies de disques P6000 EVA avec le serveur Oracle, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server et Microsoft Volume Shadow Copy Service.

Famille de baies de disques P6000 EVA intégration avec Oracle Server

Conditions préalables

- Le logiciel suivant doit être installé et configuré sur le système d'application et sur le système de sauvegarde pour la méthode ZDB de jeu de sauvegarde :
  - Oracle Enterprise Server (RDBMS)
  - Services Oracle Net
  - SQL*Plus

  Le logiciel Oracle du système de sauvegarde doit être installé sur le même répertoire que sur le système d'application. Les binaires doivent être identiques à ceux du système d'application. Vous pouvez l'obtenir en copiant les fichiers et l'environnement système du système d'application vers les système de sauvegarde, ou en effectuant une nouvelle installation 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 du système d'application doivent être installés sur les volumes sources qui seront répliqués à l'aide de l'agent SMI-S que vous avez installé.

  En fonction de l'emplacement du fichier de contrôle Oracle, des fichiers journaux de rétablissement en ligne, et Oracle SPFILE, les deux options suivantes sont possibles :
  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et Oracle SPFILE se trouvent dans un **différent** groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle.

    Par défaut, la restauration instantanée est activée pour une telle configuration.
  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et Oracle SPFILE se trouvent dans un **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* active pour une telle configuration. Vous pouvez activer la restauration instantanée en configurant les options omnirc `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Pour plus d'informations, reportez-vous à la section *Guide d'intégration Data Protector Sauvegarde avec temps d'indisponibilité nul*.

Les fichiers journaux de rétablissement archivés Oracle ne doivent pas se trouver sur les volumes sources.

Si certains des fichiers de données Oracle sont installés sur des liens symboliques, alors ces liens doivent aussi être créés sur le système de sauvegarde.

Procédure d'installation

Effectuez les tâches d'installation suivantes :

1. Installez la base de données catalogue de récupération Oracle. Installez-la de préférence sur un système séparé, sur des disques non mis en miroir. Laissez le catalogue de récupération non enregistré. Pour plus d'informations sur la manière d'installer la base de données, consultez la documentation Oracle.
2. Installez les composants logiciels Data Protector suivants :
   - `P6000 / 3PAR SMI-S Agent` – sur le système d'application et le système de sauvegarde
   - `Oracle Integration` – sur le système d'application et le système de sauvegarde

> **REMARQUE :**
> - Le composant Data Protector`Oracle Integration` du système de sauvegarde est uniquement requis pour la méthode ZDB de jeu de sauvegarde. Il n'est pas nécessaire pour la méthode ZDB Proxy Copy.
> - Dans un environnement de cluster RAC, la base de données de l'application Oracle est accessible par plusieurs instances d'Oracle. Par conséquent, installez les composants Data Protector`Oracle Integration` et `P6000 / 3PAR SMI-S Agent` sur tous les systèmes où les instances Oracle sont exécutées.
> - Si vous avez installé la base de données catalogue de récupération Oracle sur un système séparé, il n'est pas nécessaire d'y installer de composants logiciels Data Protector.

Famille de baies de disques P6000 EVA intégration avec SAP R/3

Conditions préalables

- Le logiciel Oracle suivant doit être installé 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 pas sur le système d'application), configurez le système de sauvegarde. Pour plus d'informations, consultez le guide de la base de données SAP pour Oracle

(sauvegarde Split Mirror, configuration logicielle).

- La base de données sur le système d'application peut être installée sur les images disques, les volumes logiques ou les systèmes de fichiers.
  - Les fichiers de données Oracle *doivent* se trouver sur une baie de disques.
  - Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas se trouver sur une baie de disques. Les sessions ZDB compatibles SAP *en ligne* sont une exception, pour laquelle le fichier de contrôle doit se trouver sur une baie de disques.
  - Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* se trouver sur une baie de disques.
  - Les fichiers journaux de rétablissement archivés ne doivent pas se trouver sur une baie de disques.

  Si le fichier de contrôle Oracle, les journaux de rétablissement en ligne et Oracle SPFILE se trouvent sur le même groupe de volumes LVM ou volume source en tant que fichiers de données Oracle, définissez les options Data Protector`ZDB_ORA_NO_CHECKCONF_IR`, `ZDB_ORA_INCLUDE_CF_OLF` et `ZDB_ORA_INCLUDE_SPFomnirc`. Dans le cas contraire, vous ne pouvez pas exécuter les sessions ZDB sur disque et ZDB sur disque + bande. Pour plus d'informations, voir *Guide d'intégration Data Protector Sauvegarde avec temps d'indisponibilité nul*.

  > **REMARQUE :**
  > Si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez également les liens sur le système de sauvegarde.
  >
  > ***Systèmes UNIX :*** si la base de données Oracle est installée sur les partitions brutes (Rawdisk ou volumes logiques bruts), assurez-vous que les noms du volume/groupe de disques sur le système d'application et le système de sauvegarde sont identiques.

- Sur les systèmes UNIX, assurez-vous que les utilisateurs suivants existent sur le système d'application :
  - `ora`*`ORACLE_SID`* avec 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.

  Voici une liste des répertoires standard qui doivent être installés sur le système d'application après l'installation de SAP R/3 :

  > **REMARQUE :**
  > l'emplacement des répertoires dépend des variables de l'environnement (systèmes UNIX) ou de registre (système Windows). Pour plus d'informations, reportez-vous à la documentation de SAP R/3.

  - *`ORACLE_HOME`* `/dbs` (systèmes UNIX) *`ORACLE_HOME`*`\database` (systèmes Windows) - les profils Oracle et SAP
  - *`ORACLE_HOME`* `/bin` (systèmes UNIX) *`ORACLE_HOME`*`\bin` (systèmes Windows) - les fichiers binaires Oracle

- *SAPDATA_HOME* /sapbackup (systèmes UNIX) *SAPDATA_HOME*\sapbackup (systèmes Windows) - le répertoire SAPBACKUP contenant les fichiers journaux BRBACKUP
- *SAPDATA_HOME* /saparch (systèmes UNIX) *SAPDATA_HOME*\saparch (systèmes Windows) - le répertoire SAPARCH contenant les fichiers journaux BRARCHIVE
- *SAPDATA_HOME* /sapreorg (systèmes UNIX) *SAPDATA_HOME*\sapreorg (systèmes Windows)
- *SAPDATA_HOME* /sapcheck (systèmes UNIX) *SAPDATA_HOME*\sapcheck (systèmes Windows)
- *SAPDATA_HOME* /saptrace (systèmes UNIX) *SAPDATA_HOME*\saptrace (systèmes Windows)
- /usr/sap/*ORACLE_SID*/SYS/exe/run (systèmes UNIX)

  c:\Oracle*ORACLE_SID*\sys\exe\run (systèmes Windows)

  > **REMARQUE :**
  > Si vous envisagez d'effectuer une restauration instantanée, assurez-vous que les répertoires sapbackup, saparch et sapreorg se trouvent sur différents volumes sources que les fichiers de données Oracle.

Systèmes UNIX

Sur les systèmes UNIX, si les six derniers répertoires ne se trouvent pas sur des destinations spécifiées, créez des liens appropriés vers ces répertoires.

Sur les systèmes UNIX, le répertoire /usr/sap/*ORACLE_SID*/SYS/exe/run doit être détenu par 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 jeu binaire setuid (chmod 4755 ...). L'exception est le fichier BRRESTORE, qui doit appartenir à l'utilisateur UNIX *ORACLE_SID*adm.

Exemple UNIX

Si *ORACLE_SID* est PRO, alors les permissions à l'intérieur du répertoire /usr/sap/PRO/SYS/exe/run doivent ressembler à :

```
-rwsr-xr-x 1 orapro dba 4598276 Apr 17 2011 brarchive -rwsr-xr-x 1 orapro dba
4750020 Apr 17 2011 brbackup -rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011
brconnect -rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011

brrestore -rwsr-xr-x 1 orapro dba 188629 Apr 17 2011 brtools
```

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 sur le système de sauvegarde :
   - P6000 / 3PAR SMI-S Agent

- SAP R/3 Integration
- Disk Agent

> **REMARQUE :**
> Vous devez installer SAP R/3 Integration sur le système de sauvegarde, uniquement si vous envisagez d'exécuter des sessions ZDB compatibles SAP dans lesquelles BRBACKUP est démarré sur le système de sauvegarde.
>
> Sur les systèmes Windows, les composants logiciels Data Protector doivent être installés à l'aide du compte utilisateur de l'administrateur SAP R/3, et ce compte doit être inclus dans le groupe local ORA_DBA ou ORA_*SID*_DBA sur le système dans lequel l'instance SAP R/3 est en cours d'exécution.

Famille de baies de disques P6000 EVA intégration avec Microsoft Exchange Server

Conditions préalables

La base de données Microsoft Exchange Server doit être installée sur les volumes sources du système d'application. Les objets suivants doivent être situés sur les volumes sources :

- Microsoft Information Store (MIS)
- en option, Key Management Service (KMS)
- en option, Site Replication Service (SRS)

Afin de pouvoir sauvegarder les journaux de transaction, désactivez l'enregistrement circulaire sur Microsoft Exchange Server.

Procédure d'installation

Installez les composants logiciels Data Protector suivants :

- P6000 / 3PAR SMI-S Agent – à la fois sur le système d'application et le système de sauvegarde
- MS Exchange Integration – sur le système d'application uniquement

Famille de baies de disques P6000 EVA intégration avec Microsoft SQL Server

Conditions préalables

Microsoft SQL Server doit être installé sur le système d'application. Les base de données utilisateur *doivent* se trouver sur les volumes sources de la baie de disques, alors que les bases de données du système peuvent être installées n'importe où ailleurs. Cependant, si les bases de données du système sont également installées sur la baie de disques, elles *doivent* être installées sur des volumes sources *différents* que ceux des bases de données utilisateur.

Procédure d'installation

Installez les composants logiciels Data Protector suivants sur le système d'application et sur le système de sauvegarde :

- `P6000 / 3PAR SMI-S Agent` – à la fois sur le système d'application et le système de sauvegarde
- `MS SQL Integration` – sur le système d'application uniquement

Famille de baies de disque P9000 XP clients

Pour intégrer Famille de baies de disque P9000 XP avec Data Protector, installez les composants logiciels Data Protector suivants sur l'application et les systèmes de sauvegarde :

- `P9000 XP Agent`
- `General Media Agent`

  Installez le composant `General Media Agent` sur le système de sauvegarde afin de sauvegarder les données de masse. Installez-le sur le système d'application afin de sauvegarder les journaux d'archive ou d'effectuer une restauration sur le système d'application.
- `Disk Agent`

  Installez le composant `Disk Agent` sur l'application et les systèmes de sauvegarde afin d'exécuter la sauvegarde avec temps d'indisponibilité nul des systèmes de fichiers ou images de disques. Les clients ne disposant pas de l'agent de disque ne sont pas répertoriés dans les listes déroulantes `Application system` et `Backup system` pendant la création d'une spécification de sauvegarde ZDB.

> **IMPORTANT :**
> Sur les systèmes Microsoft Windows Server 2008, deux correctifs Windows Server 2008 doivent être installés afin d'activer le fonctionnement normal de l'intégration Data Protector Famille de baies de disque P9000 XP. Vous pouvez télécharger les packages de correctifs nécessaires sur les sites Web de Microsoft http://support.microsoft.com/kb/952790 et http://support.microsoft.com/kb/971254.
>
> Cette condition supplémentaire ne s'applique pas aux systèmes Windows Server 2008 R2.

Installation dans un cluster

Vous pouvez installer l'intégration Famille de baies de disque P9000 XP dans un environnement de cluster. Pour connaître les configurations de cluster prises en charge et les conditions spécifiques d'installation, consultez le *Guide de l'administrateur Data Protector Sauvegarde avec temps d'indisponibilité nul*.

Intégration avec d'autres applications

Pour installer l'intégration Famille de baies de disque P9000 XP avec une application de base de données, installez le composant Data Protector spécifique à l'intégration particulière sur l'application et les systèmes de sauvegarde, et effectuez les tâches d'installation spécifiques à cette intégration.

Vous pouvez installer l'intégration Famille de baies de disque P9000 XP avec le serveur Oracle, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server et Microsoft Volume Shadow Copy Service.

Famille de baies de disque P9000 XP intégration avec Oracle Server

Conditions préalables

- Le logiciel suivant doit être installé et configuré sur le système d'application et sur le système de sauvegarde pour la méthode ZDB de jeu de sauvegarde :
  - Oracle Enterprise Server (RDBMS)
  - Services Oracle Net
  - SQL*Plus

  Le logiciel Oracle du système de sauvegarde doit être installé sur le même répertoire que sur le système d'application. Les binaires doivent être identiques à ceux du système d'application. Vous pouvez l'obtenir en copiant les fichiers et l'environnement système du système d'application vers les système de sauvegarde, ou en effectuant une nouvelle installation 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 les LDEV Famille de baies de disque P9000 XP qui sont mis en miroir sur le système de sauvegarde.

  Dans le cas de la méthode de jeu de sauvegarde, si certains des fichiers de données Oracle sont installés sur des liens symboliques, alors ces liens doivent aussi être créés sur le système de sauvegarde.

  En fonction de l'emplacement du fichier de contrôle Oracle, des fichiers journaux de rétablissement en ligne, et Oracle SPFILE, les deux options suivantes sont possibles :
  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et Oracle SPFILE se trouvent dans un **différent** groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle.

    Par défaut, la restauration instantanée est activée pour une telle configuration.
  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et Oracle SPFILE se trouvent dans un **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* active pour une telle configuration. Vous pouvez activer la restauration instantanée en configurant les options omnirc `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF` et `ZDB_ORA_NO_CHECKCONF_IR`. Pour plus d'informations, reportez-vous à la section *Guide d'intégration Data Protector Sauvegarde avec temps d'indisponibilité nul*.

  Les fichiers journaux de rétablissement archivés Oracle ne doivent pas se trouver sur les volumes sources.

Procédure d'installation

Effectuez les tâches d'installation suivantes :

1. Installez la base de données catalogue de récupération Oracle. Installez-la de préférence sur un système séparé, sur des disques non mis en miroir. Laissez le catalogue de récupération non enregistré. Pour plus d'informations sur la manière d'installer la base de données, consultez la documentation Oracle.
2. Installez les composants logiciels Data Protector suivants :
   - `P9000 XP Agent` – sur le système d'application et le système de sauvegarde
   - `Oracle Integration` – sur le système d'application et le système de sauvegarde

> **REMARQUE :**
> - Le composant `Oracle Integration` Data Protectordu système de sauvegarde est uniquement requis pour la méthode ZDB de jeu de sauvegarde. Il n'est pas nécessaire pour la méthode ZDB Proxy Copy.
> - Dans un environnement de cluster RAC, la base de données de l'application Oracle est accessible par plusieurs instances d'Oracle. Par conséquent, installez les composants `Oracle Integration` Data Protectoret `P9000 XP Agent` sur tous les systèmes où les instances Oracle sont exécutées.
> - Si vous avez installé la base de données catalogue de récupération Oracle sur un système séparé, il n'est pas nécessaire d'y installer de composants logiciels Data Protector.

Famille de baies de disque P9000 XP intégration avec SAP R/3

Conditions préalables

- Le logiciel Oracle suivant doit être installé et configuré 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 pas sur le système d'application), configurez le système de sauvegarde. Pour plus d'informations, consultez le guide de la base de données SAP pour Oracle (sauvegarde Split Mirror, configuration logicielle).
- La base de données sur le système d'application peut être installée sur les images disques, les volumes logiques ou les systèmes de fichiers.

- Les fichiers de données Oracle *doivent* se trouver sur une baie de disques.
- Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas se trouver sur une baie de disques. Les sessions ZDB compatibles SAP *en ligne* sont une exception, pour laquelle le fichier de contrôle doit se trouver sur une baie de disques.
- Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* se trouver sur une baie de disques.
- Les fichiers journaux de rétablissement archivés ne doivent pas se trouver sur une baie de disques.

Si le fichier de contrôle Oracle, les journaux de rétablissement en ligne et Oracle SPFILE se trouvent sur le même groupe de volumes LVM ou volume source en tant que fichiers de données Oracle, définissez les options Data Protector`ZDB_ORA_NO_CHECKCONF_IR`, `ZDB_ORA_INCLUDE_CF_OLF` et `ZDB_ORA_INCLUDE_SPFomnirc`. Dans le cas contraire, vous ne pouvez pas exécuter les sessions ZDB sur disque et ZDB sur disque + bande. Pour plus d'informations, voir *Guide d'intégration Data Protector Sauvegarde avec temps d'indisponibilité nul*.

> **REMARQUE :**
> Si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez également les liens sur le système de sauvegarde.
>
> ***Systèmes UNIX :*** si la base de données Oracle est installée sur les partitions brutes (Rawdisk ou volumes logiques bruts), assurez-vous que les noms du volume/groupe de disques sur le système d'application et le système de sauvegarde sont identiques.

- Sur les systèmes UNIX, assurez-vous que les utilisateurs suivants existent sur le système d'application :
  - `ora`*`ORACLE_SID`* avec 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.

  Voici une liste des répertoires standard qui doivent être installés sur le système d'application après l'installation de SAP R/3 :

  > **REMARQUE :**
  > l'emplacement des répertoires dépend des variables de l'environnement (systèmes UNIX) ou du registre (système Windows). Pour plus d'informations, reportez-vous à la documentation de SAP R/3.

  - *`ORACLE_HOME`* `/dbs` (systèmes UNIX)

    ORACLE_HOME `\database` (systèmes Windows) - les profils Oracle et SAP R/3
  - *`ORACLE_HOME`* `/bin or` (systèmes UNIX)

    ORACLE_HOME `\bin` (systèmes Windows) - les binaires Oracle
  - *`SAPDATA_HOME`* `/sapbackup` (systèmes UNIX)

    SAPDATA_HOME `\sapbackup` (systèmes Windows) - le

répertoire SAPBACKUP avec les fichiers journaux BRBACKUP

- *SAPDATA_HOME* /saparch (systèmes UNIX)
  SAPDATA_HOME \saparch (systèmes Windows) - le répertoire SAPARCH avec les fichiers journaux BRARCHIVE
- *SAPDATA_HOME* /sapreorg (systèmes UNIX)
  SAPDATA_HOME \sapreorg (systèmes Windows)
- *SAPDATA_HOME* /sapcheck (systèmes UNIX)
  SAPDATA_HOME \sapcheck (systèmes Windows)
- *SAPDATA_HOME* /saptrace (systèmes UNIX)
  SAPDATA_HOME \saptrace (systèmes Windows)
- /usr/sap/*ORACLE_SID*/SYS/exe/run (systèmes UNIX)
  c:\Oracle*ORACLE_SID*\sys\exe\run (systèmes Windows)

  > **REMARQUE :**
  > Si vous envisagez d'effectuer une restauration instantanée, assurez-vous que les répertoires sapbackup, saparch et sapreorg se trouvent sur différents volumes sources que les fichiers de données Oracle.

Systèmes UNIX

Sur les systèmes UNIX, si les six derniers répertoires ne se trouvent pas sur des destinations spécifiées, créez des liens appropriés vers ces répertoires.

Sur les systèmes UNIX, le répertoire /usr/sap/*ORACLE_SID*/SYS/exe/run doit être détenu par 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 jeu binaire setuid (chmod 4755 ...). L'exception est le fichier BRRESTORE, qui doit appartenir à l'utilisateur UNIX *ORACLE_SID*adm.

Exemple UNIX

Si *ORACLE_SID* est PRO, alors les permissions à l'intérieur du répertoire /usr/sap/PRO/SYS/exe/run doivent ressembler à :

```
-rwsr-xr-x 1 orapro dba 4598276 Apr 17 2011 brarchive -rwsr-xr-x 1 orapro dba
4750020 Apr 17 2011 brbackup -rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011
brconnect -rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011

brrestore -rwsr-xr-x 1 orapro dba 188629 Apr 17 2011 brtools
```

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 sur le système de sauvegarde :

- P9000 XP Agent
- SAP R/3 Integration
- Disk Agent

> **REMARQUE :**
> Vous devez installer SAP R/3 Integration sur le système de sauvegarde, uniquement si vous envisagez d'exécuter des sessions ZDB compatibles SAP dans lesquelles BRBACKUP est démarré sur le système de sauvegarde.
>
> Sur les systèmes Windows, les composants logiciels Data Protector doivent être installés à l'aide du compte utilisateur de l'administrateur SAP R/3, et ce compte doit être inclus dans le groupe local ORA_DBA ou ORA_*SID*_DBA sur le système dans lequel l'instance SAP R/3 est en cours d'exécution.

Famille de baies de disque P9000 XP intégration avec Microsoft Exchange Server

Conditions préalables

La base de données de Microsoft Exchange Server doit être installée sur le système d'application sur les volumes (LDEV)Famille de baies de disque P9000 XP, qui sont mis en miroir sur le système de sauvegarde. La mise en miroir peut être Business Copy P9000 XP ou Continuous Access P9000 XP et la base de données installée sur un système de fichiers. Les objets suivants doivent être situés sur les volumes qui sont mis en miroir :

- Microsoft Information Store (MIS)
- en option, Key Management Service (KMS)
- en option, Site Replication Service (SRS)

Afin de pouvoir sauvegarder les journaux de transaction, désactivez l'enregistrement circulaire sur Microsoft Exchange Server.

Procédure d'installation

Installez les composants logiciels Data Protector suivants :

- P9000 XP Agent – sur le système d'application et de sauvegarde
- MS Exchange Integration – sur le système d'application uniquement

Famille de baies de disque P9000 XP intégration avec Microsoft SQL Server

Conditions préalables

Microsoft SQL Server doit être installé sur le système d'application. Les base de données utilisateur *doivent* se trouver sur les volumes sources de la baie de disques, alors que les bases de données du système peuvent être installées n'importe où ailleurs. Cependant, si les bases de données du système sont également installées sur la baie de disques, elles *doivent* être installées sur des volumes sources *différents* que ceux des bases de données utilisateur.

Procédure d'installation

Installez les composants logiciels Data Protector suivants sur le système d'application et sur le système de sauvegarde :

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

3PAR StoreServ Storage clients

Pour intégrer 3PAR StoreServ Storage avec Data Protector, installez les composants logiciels Data Protector suivants sur les systèmes d'application et de sauvegarde :

- `P6000 / 3PAR SMI-S Agent`

Pour la sauvegarde et la restauration des objets à l'aide de Volume Shadow Copy Service, vous avez également besoin des composants suivants :

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

Quel que soit le système d'exploitation, pour effectuer des sessions ZDB sur disque + bande ou ZDB sur bande, installez en plus le composant logiciel Data Protector suivant sur le système de sauvegarde :

- `General Media Agent`

Clients EMC Symmetrix

Pour intégrer EMC Symmetrix avec Data Protector, installez les composants logiciels Data Protector suivants sur les systèmes d'application et de sauvegarde :

- `EMC Symmetrix Agent` (SYMA)

  Avant d'installer à distance le composant `EMC Symmetrix Agent`, installez les deux composants EMC suivants :

- Outil de solution EMC
- Microcode ou licence EMC Symmetrix TimeFinder ou EMC Symmetrix Remote Data Facility (SRDF).

- `General Media Agent`

  Installez le composant `General Media Agent` sur le système de sauvegarde afin de sauvegarder les données de masse. Installez-le sur le système d'application afin de sauvegarder les journaux d'archive ou d'effectuer une restauration sur le système d'application.
- `Disk Agent`

  Installez le composant `Disk Agent` sur les systèmes d'application et de sauvegarde afin d'exécuter l'image de disque et le ZDB de système de fichiers. Les clients ne disposant pas de l'agent de disque ne sont pas répertoriés dans les listes déroulantes `Application system` et `Backup system` pendant la création d'une spécification de sauvegarde ZDB.

Installation dans un cluster

Vous pouvez installer l'intégration EMC Symmetrix dans un environnement de cluster. Pour connaître les configurations de cluster prises en charge et les conditions spécifiques d'installation, consultez le *Guide de l'administrateur Data Protector Sauvegarde avec temps d'indisponibilité nul*.

Intégration avec d'autres applications

Pour installer l'intégration EMC Symmetrix avec une application de base de données, installez le composant Data Protector spécifique à l'intégration particulière sur l'application et les systèmes de sauvegarde, et effectuez les tâches d'installation spécifiques à cette intégration. Vous pouvez installer l'intégration EMC Symmetrix avec Oracle et SAP R/3.

Intégration EMC Symmetrix avec Oracle

Conditions préalables

- Le logiciel suivant doit être installé et configuré 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 les périphériques EMC Symmetrix qui sont mis en miroir sur le système de sauvegarde.

  La base de données peut être installée sur les images disques, les volumes logiques ou les 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 se trouver sur des disques non mis en miroir.

Procédure d'installation

Effectuez les tâches d'installation suivantes :

1. Installez la base de données catalogue de récupération Oracle. Installez-la de préférence sur un système séparé, sur des disques non mis en miroir. Laissez le catalogue de récupération non enregistré. Pour plus d'informations sur la manière d'installer la base de données, consultez la documentation Oracle.
2. Installez les composants logiciels Data Protector suivants :
   - `EMC Symmetrix Agent` – sur le système d'application et le système de sauvegarde
   - `Oracle Integration` – sur le système d'application et le système de sauvegarde

   REMARQUE :
   - Le composant Data Protector`Oracle Integration` du système de sauvegarde est uniquement requis pour la méthode ZDB de jeu de sauvegarde. Il n'est pas nécessaire pour la méthode ZDB Proxy Copy.
   - Dans un environnement de cluster RAC, la base de données de l'application Oracle est accessible par plusieurs instances d'Oracle. Par conséquent, installez les composants Data Protector`Oracle Integration` et `EMC Symmetrix Agent` sur tous les systèmes où les instances Oracle sont exécutées.
   - Si vous avez installé la base de données catalogue de récupération Oracle sur un système séparé, il n'est pas nécessaire d'y installer de composants logiciels Data Protector.

Intégration EMC Symmetrix avec SAP R/3

Conditions préalables

- Le logiciel Oracle suivant doit être installé et configuré 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 pas sur le système d'application), configurez le système de sauvegarde. Pour plus d'informations, consultez le guide de la base de données SAP pour Oracle (sauvegarde Split Mirror, configuration logicielle).

- La base de données sur le système d'application peut être installée sur les images disques, les volumes logiques ou les systèmes de fichiers.
  - Les fichiers de données Oracle *doivent* se trouver sur une baie de disques.
  - Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas se trouver sur une baie de disques. Les sessions ZDB compatibles SAP *en ligne* sont une exception, pour laquelle le fichier de contrôle doit se trouver sur une baie de disques.
  - Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* se trouver sur une baie de disques.
  - Les fichiers journaux de rétablissement archivés ne doivent pas se trouver sur une baie de disques.

  > **REMARQUE :**
  > Si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez également les liens sur le système de sauvegarde.
  >
  > ***Systèmes UNIX :*** si la base de données Oracle est installée sur les partitions brutes (Rawdisk ou volumes logiques bruts), assurez-vous que les noms du volume/groupe de disques sur le système d'application et le système de sauvegarde sont identiques.

- Sur les systèmes UNIX, assurez-vous que les utilisateurs suivants existent sur le système d'application :
  - ora*ORACLE_SID* avec 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.

  Voici une liste des répertoires standard qui 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. Pour plus d'informations, reportez-vous à la documentation de SAP R/3.

  - *ORACLE_HOME* `/dbs` - les profils Oracle et SAP R/3
  - *ORACLE_HOME* `/bin` - les fichiers binaires Oracle
  - *SAPDATA_HOME* `/sapbackup` - répertoire SAPBACKUP contenant les fichiers journaux BRBACKUP
  - *SAPDATA_HOME* `/saparch` - 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, assurez-vous que les répertoires sapbackup, saparch et sapreorg se trouvent sur différents volumes sources que les fichiers de données Oracle.

Si les six derniers répertoires ne se trouvent pas sur des destinations spécifiées, créez des liens appropriés vers ces répertoires.

Le répertoire /usr/sap/*ORACLE_SID*/SYS/exe/run doit être détenu par 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 jeu binaire setuid (chmod 4755 ...). L'exception est le fichier BRRESTORE, qui doit appartenir à l'utilisateur UNIX *ORACLE_SID*adm.

Exemple

Si *ORACLE_SID* est PRO, alors les permissions à l'intérieur du répertoire /usr/sap/PRO/SYS/exe/run doivent ressembler à :

```
-rwsr-xr-x 1 orapro dba 4598276 Apr 17 2011 brarchive -rwsr-xr-x 1 orapro dba
4750020 Apr 17 2011 brbackup -rwsr-xr-x 1 orapro dba 4286707 Apr 17 2011
brconnect -rwsr-xr-x 1 proadm sapsys 430467 Apr 17 2011 brrestore -rwsr-xr-x 1
orapro dba 188629 Apr 17 2011 brtools
```

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 sur le système de sauvegarde :
   - EMC Symmetrix Agent
   - SAP R/3 Integration
   - Disk Agent

> **REMARQUE :**
> Vous devez installer SAP R/3 Integration sur le système de sauvegarde, uniquement si vous envisagez d'exécuter des sessions ZDB compatibles SAP dans lesquelles BRBACKUP est démarré sur le système de sauvegarde.

Intégration EMC Symmetrix avec Microsoft SQL Server

Conditions préalables

Microsoft SQL Server doit être installé sur le système d'application. Les base de données utilisateur *doivent* se trouver sur les volumes sources de la baie de disques, alors que les bases de données du système peuvent être installées n'importe où ailleurs. Cependant, si les bases de données du système sont également installées sur la baie de disques, elles *doivent* être installées sur des volumes sources *différents* que ceux des bases de données utilisateur.

Procédure d'installation

Installez les composants logiciels Data Protector suivants sur le système d'application et sur le système de sauvegarde :

- `EMC Symmetrix Agent`
- `MS SQL Integration`

Baies de stockage non HPE

Data Protector utilise des fournisseurs de stockage pour les baies de stockage non HPE afin de s'intégrer aux baies de stockage ZDB suivantes : stockage NetApp, gammes de stockage EMC VNX et EMC VMAX. Ce composant Fournisseur de stockage est un module d'extension de l'Agent Data Protector SMI-S. Il active la fonctionnalité ZDB pour le stockage respectif par le biais de l'agent SMI-S.

Installez les composants logiciels Data Protector suivants sur le système d'application et sur le système de sauvegarde :

- L'un des composants Fournisseur de stockage pour les baies de stockage non HPE selon le stockage que vous utilisez (`NetApp Storage Provider`, `EMC VNX Storage Provider`, ou `EMC VMAX Storage Provider`)

Pour effectuer des sessions ZDB sur bande, installez le composant logiciel Data Protector suivant sur le système de sauvegarde :

- `General Media Agent`

Intégration avec d'autres applications

Pour installer l'intégration Storage Array Data Protector non HPE avec une application de la base de données ou une intégration d'environnement virtuel, installez le composant Data Protector spécifique à l'intégration particulière sur les systèmes applicables et effectuez les tâches d'intégration spécifiques à cette intégration. Vous pouvez installer l'intégration Storage Array non HPE avec VMware, Oracle Server, SAP R/3 et Microsoft SQL Server. Reportez-vous aux dernières matrices de prise en charge sur https://softwaresupport.softwaregrp.com/ pour savoir quelles combinaisons des baies de stockage non HPE avec les applications de base de données spécifiques ou une intégration d'environnement virtuel sont prises en charge.

Intégration Storage Array non HPE avec l'environnement virtuel pour VMware

Limites

- Seul l'environnement VMware vCenter est pris en charge.
- La restauration instantanée n'est pas prise en charge.
- Seule la sauvegarde ZDB sur bande est prise en charge.

Conditions préalables

Tous les systèmes sur lesquels vous essayez d'installer les composants sont opérationnels.

Procédure d'installation

Sur les systèmes qui doivent contrôler les sessions de sauvegarde et de restauration (système de sauvegarde), installez les composants Data Protector suivants :

- `Virtual Environment Integration`
- Fournisseur de stockage pour la baie de stockage non HPE (`NetApp Storage Provider`)
- `General Media Agent`
- `Disk Agent`

> **REMARQUE :**
> - Le composant `Disk Agent` vous permet d'utiliser le bouton **Parcourir** lors de la restauration vers un répertoire sur l'hôte de sauvegarde. Si le composant n'est pas installé, vous devez tapez le répertoire cible vous-même.
> - Le client que vous essayez d'utiliser comme hôte de sauvegarde *ne doit pas* disposer du logiciel de sauvegarde consolidée VMware (VCB) installé.

Intégration Storage Array non HPE avec Oracle Server

Limites

- L'environnement de cluster RAC n'est pas pris en charge.
- La restauration instantanée n'est pas prise en charge.
- Seule la sauvegarde ZDB sur bande est prise en charge.

Conditions préalables

- Le logiciel suivant doit être installé et configuré sur le système d'application et sur le système de sauvegarde pour la méthode ZDB de jeu de sauvegarde :

- Oracle Enterprise Server (RDBMS)
- Services Oracle Net
- SQL*Plus

Le logiciel Oracle du système de sauvegarde doit être installé sur le même répertoire que sur le système d'application. Les binaires doivent être identiques à ceux du système d'application. Vous pouvez l'obtenir en copiant les fichiers et l'environnement système du système d'application vers les système de sauvegarde, ou en effectuant une nouvelle installation 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 du système d'application doivent être installés sur les volumes sources qui seront répliqués à l'aide du fournisseur de stockage (par le biais de l'agent SMI-S) que vous avez installé.

  En fonction de l'emplacement du fichier de contrôle Oracle, des fichiers journaux de rétablissement en ligne, et Oracle SPFILE, les deux options suivantes sont possibles :

  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et Oracle SPFILE se trouvent dans un **différent** groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle.
  - Le fichier de contrôle Oracle, les fichiers journaux de rétablissement en ligne et Oracle SPFILE se trouvent dans un **même** groupe de volumes (si LVM est utilisé) ou volume source que les fichiers de données Oracle.

  Les fichiers journaux de rétablissement archivés Oracle ne doivent pas se trouver sur les volumes sources.

  Si certains des fichiers de données Oracle sont installés sur des liens symboliques, alors ces liens doivent aussi être créés sur le système de sauvegarde.

Procédure d'installation

Effectuez les tâches d'installation suivantes :

1. Installez la base de données catalogue de récupération Oracle. Installez-la de préférence sur un système séparé, sur des disques non mis en miroir. Laissez le catalogue de récupération non enregistré. Pour plus d'informations sur la manière d'installer la base de données, consultez la documentation Oracle.
2. Installez les composants logiciels Data Protector suivants :
   - Fournisseur de stockage pour la baie de stockage non HPE (`NetApp Storage Provider`, `EMC VNX Storage Provider`, ou `EMC VMAX Storage Provider`) – sur le système d'application et le système de sauvegarde
   - `Oracle Integration` – sur le système d'application et le système de sauvegarde

   > **REMARQUE :**
   > - Le composant Data Protector`Oracle Integration` du système de sauvegarde est uniquement requis pour la méthode ZDB de jeu de sauvegarde. Il n'est pas nécessaire pour la méthode ZDB Proxy Copy.

> - Si vous avez installé la base de données catalogue de récupération Oracle sur un système séparé, il n'est pas nécessaire d'y installer de composants logiciels Data Protector.

Intégration Storage Array non HPE avec SAP R/3

Limites

- La restauration instantanée n'est pas prise en charge.
- Seule la sauvegarde ZDB sur bande est prise en charge.

Conditions préalables

- Le logiciel Oracle suivant doit être installé 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 pas sur le système d'application), configurez le système de sauvegarde. Pour plus d'informations, consultez le guide de la base de données SAP pour Oracle (sauvegarde Split Mirror, configuration logicielle).
- La base de données sur le système d'application peut être installée sur les images disques, les volumes logiques ou les systèmes de fichiers.
  - Les fichiers de données Oracle *doivent* se trouver sur un système de stockage.
  - Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne ne doivent pas se trouver sur un système de stockage. Les sessions ZDB compatibles SAP *en ligne* sont une exception, pour laquelle le fichier de contrôle doit se trouver sur un système de stockage.
  - Pour la *sauvegarde en ligne*, le fichier de contrôle et les journaux de rétablissement en ligne *doivent* se trouver sur un système de stockage.
  - Les fichiers journaux de rétablissement archivés ne doivent pas se trouver sur un système de stockage.

> **REMARQUE :**
> Si certains des fichiers de données Oracle sont installés sur des liens symboliques, créez également les liens sur le système de sauvegarde.
>
> ***Systèmes UNIX :*** Si la base de données Oracle est installée sur les partitions brutes (Rawdisk ou volumes logiques bruts), assurez-vous que les noms du volume/groupe de disques sur le système d'application et le système de sauvegarde sont identiques.

- Sur les systèmes UNIX, assurez-vous que les utilisateurs suivants existent sur le système d'application :
  - ora*ORACLE_SID* avec 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.

  Voici une liste des répertoires standard qui doivent être installés sur le système d'application après l'installation de SAP R/3 :

  > **REMARQUE :**
  > l'emplacement des répertoires dépend des variables de l'environnement (systèmes UNIX) ou de registre (système Windows). Pour plus d'informations, reportez-vous à la documentation de SAP R/3.

  - *ORACLE_HOME* /dbs (systèmes UNIX) *ORACLE_HOME*\database (systèmes Windows) - les profils Oracle et SAP
  - *ORACLE_HOME* /bin(systèmes UNIX) *ORACLE_HOME*\bin(systèmes Windows) - les fichiers binaires Oracle
  - *SAPDATA_HOME* /sapbackup(systèmes UNIX) *SAPDATA_HOME*\sapbackup (systèmes Windows) - le répertoire SAPBACKUP contenant les fichiers journaux BRBACKUP
  - *SAPDATA_HOME* /saparch(systèmes UNIX) *SAPDATA_HOME*\saparch (systèmes Windows) - le répertoire SAPARCH contenant les fichiers journaux BRARCHIVE
  - *SAPDATA_HOME* /sapreorg (systèmes UNIX) *SAPDATA_HOME* \sapreorg(systèmes Windows)
  - *SAPDATA_HOME* /sapcheck (systèmes UNIX) *SAPDATA_HOME* \sapcheck(systèmes Windows)
  - *SAPDATA_HOME* /saptrace(systèmes UNIX) *SAPDATA_HOME*\saptrace (systèmes Windows)
  - /usr/sap/*ORACLE_SID*/SYS/exe/run (systèmes UNIX)

    c:\Oracle*ORACLE_SID*\sys\exe\run (systèmes Windows)

  Systèmes UNIX

  Sur les systèmes UNIX, si les six derniers répertoires ne se trouvent pas sur des destinations spécifiées, créez des liens appropriés vers ces répertoires.

  Sur les systèmes UNIX, le répertoire /usr/sap/*ORACLE_SID*/SYS/exe/run doit être détenu par 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 jeu binaire setuid (chmod 4755 ...). L'exception est le fichier BRRESTORE, qui doit appartenir à l'utilisateur UNIX *ORACLE_SID*adm.

  Exemple UNIX

  Si *ORACLE_SID* est PRO, alors les permissions à l'intérieur du répertoire /usr/sap/PRO/SYS/exe/run doivent ressembler à :

```
-rwsr-xr-x   1 orapro dba 4598276 Apr 17  2011 brarchive
-rwsr-xr-x   1 orapro dba 4750020 Apr 17  2011 brbackup
-rwsr-xr-x   1 orapro dba 4286707 Apr 17  2011 brconnect
-rwsr-xr-x   1 proadm sapsys 430467 Apr 17  2011
brrestore
-rwsr-xr-x   1 orapro dba 188629 Apr 17  2011 brtools
```

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 sur le système de sauvegarde :
   - Fournisseur de stockage pour les baies de stockage autres que (`NetApp Storage Provider`)
   - `SAP R/3 Integration`
   - `Disk Agent`

> **REMARQUE :**
> Vous devez installer `SAP R/3 Integration` sur le système de sauvegarde, uniquement si vous envisagez d'exécuter des sessions ZDB compatibles SAP dans lesquelles BRBACKUP est démarré sur le système de sauvegarde.
>
> Sur les systèmes Windows, les composants logiciels Data Protector doivent être installés à l'aide du compte utilisateur de l'administrateur SAP R/3, et ce compte doit être inclus dans le groupe local `ORA_DBA` ou `ORA_`*`SID`*`_DBA` sur le système dans lequel l'instance SAP R/3 est en cours d'exécution.

Intégration Storage Array non HPE avec Microsoft SQL Server

Limites

- La restauration instantanée n'est pas prise en charge.
- Seule la sauvegarde ZDB sur bande est prise en charge.

Conditions préalables

Microsoft SQL Server doit être installé sur le système d'application. Les base de données utilisateur *doivent* se trouver sur les volumes sources de la baie de disques, alors que les bases de données du système peuvent être installées n'importe où ailleurs. Cependant, si les bases de données du système sont également installées sur la baie de disques, elles *doivent* être installées sur des volumes sources *différents* que ceux des bases de données utilisateur.

Procédure d'installation

Installez les composants logiciels Data Protector suivants sur le système d'application et sur le système de sauvegarde :

- Fournisseur de stockage pour la baie de stockage non HPE (`NetApp Storage Provider`, `EMC VNX Storage Provider`, ou `EMC VMAX Storage Provider`) – sur les systèmes d'application et de sauvegarde
- `MS SQL Integration` – sur le système d'application uniquement

Chapitre 5: Installation de Data Protector sur les Clusters

Installation de Data Protector sur Serviceguard

Data Protector prend en charge Serviceguard (SG) pour HP-UX et Linux. Pour obtenir des informations sur les versions de systèmes d'exploitation prises en charge, consultez Annonces sur les produits, notes sur les logiciels et références 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.

Etapes de la configuration

1. Configuration du Gestionnaire de cellule primaire
2. Configuration du Gestionnaire de cellule secondaire
3. Configuration du package Gestionnaire de cellule

Installation d'un Gestionnaire de cellule compatible cluster

Conditions préalables

Avant d'installer un Data Protector Gestionnaire de cellule sur HP Serviceguard, vérifiez ce qui suit :

- Décidez quel système va être le Gestionnaire de cellule principal et celui/ceux qui va/vont être le(s) Gestionnaire de cellule secondaire(s). Serviceguard doit être installé sur tous ces systèmes, qui doivent également être configurés en tant que membres de cluster.
- Vous devez installer le Data Protector Gestionnaire de cellule, avec les correctifs et tous les autres composants logiciels Data Protector recommandés pour les intégrations voulues dans le cluster, sur le nœud principal et sur chacun des nœuds secondaires.
- Le groupe d'utilisateurs `hpdp` et le compte utilisateur dédié `hpdp` doivent avoir les mêmes ID sur les deux nœuds.
- Dans cet environnement de cluster, un Gestionnaire de cellule Data Protector doit avoir son propre package. Avant d'installer le Gestionnaire de cellule Data Protector dans Serviceguard, vous devez obtenir les informations suivantes auprès de votre administrateur réseau :
  - Nom du serveur virtuel (le nom d'hôte spécifié dans le package du cluster)
  - Adresse IP du package ou du serveur virtuel

  De plus, vous devrez créer un groupe de volumes sur un disque partagé. Pour plus d'informations, reportez-vous à Exemple de création de groupe de volumes, Page 171.
- Vérifiez que les nœuds de cluster et l'adresse IP (virtuelle) du package figurent dans le même sous-

réseau.

- Si vous disposez du service DNS dans votre environnement, vérifiez que tous les nœuds dans le cluster, ainsi que l'adresse IP du package sont enregistrés auprès du serveur DNS.

Configuration du Gestionnaire de cellule principal

Procédure

1. Démarrez le cluster :

   ```
   cmruncl
   ```

2. Activez le groupe de volumes.

   HP-UX :

   ```
   vgchange -a e vg_name
   ```

   Linux :

   ```
   vgchange -a y vg_name
   ```

3. Montez le volume logique dans le répertoire du point de montage (par exemple, `/omni_shared`).

   ```
   mount lv_path /omni_shared
   ```

4. Modifiez le fichier de modèle `/etc/opt/omni/server/sg/sg.conf`.

   > **REMARQUE :**
   > L'option `SHARED_DISK_ROOT` doit contenir le nom de votre répertoire de point de montage (par exemple, `SHARED DISK ROOT=/omni_shared`).
   >
   > L'option `CS_SERVICE_HOSTNAME` doit contenir le nom du Gestionnaire de cellule virtuel, tel qu'il est connu sur le réseau. Chaque package du cluster nécessite sa propre adresse IP virtuelle et son nom de réseau (par exemple, `CS_SERVICE HOSTNAME=ob2cl.company.com`).

5. Configurez le Gestionnaire de cellule principal. 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 de ne pas avoir monté de sous-répertoire dans `/etc/opt/omni/` ou `/var/opt/omni/`. Exécutez :

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

   Notez que, après l'exécution de ce script, les services Data Protector sont arrêtés et seront redémarrés ultérieurement.

6. Démontez le répertoire du point de montage :

   ```
   umount dirname
   ```

7. Désactiver le groupe de volumes :

   ```
   vgchange -a n vg_name
   ```

Configuration du Gestionnaire de cellule secondaire

Procédure

1. Activez le groupe de volumes.

   HP-UX :

   `vgchange -a e vg_name`

   Linux :

   `vgchange -a y vg_name`
2. Montez le volume logique dans le répertoire du point de montage.

   `mount lv_path /omni_shared`
3. Configurez le Gestionnaire de cellule secondaire :

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

   où *dirname* est le point de montage ou répertoire partagé (par exemple`/omni_shared`).
4. Démontez le répertoire du point de montage :

   `umount /omni_shared`
5. Désactiver le groupe de volumes :

   `vgchange -a n vg_name`

Configuration du package Gestionnaire de cellule

Conditions préalables

- Le Gestionnaire de cellule Data Protector doit être installé et configuré sur les deux nœuds cluster.
- Avant de configurer le package de cluster Data Protector, vous devez avoir créé et modifié un fichier de configuration de cluster.

La configuration des packages existants inclut toujours 2 fichiers : le fichier de configuration du package et le script de contrôle du package. Le fichier de configuration du package est créé sous forme de fichier ASCII, puis stocké dans la configuration binaire Serviceguard à l'aide de la commande `cmapplyconf`. Le fichier de configuration de package modulaire contient en un seul fichier tous les systèmes de fichiers, points de montage et définitions de service du package. Ce fichier est stocké dans la configuration binaire Serviceguard à l'aide de la commande `cmapplyconf`.

> **REMARQUE :**
> Les démons Data Protector ne sont plus exécutés sur aucun des nœuds cluster.

Procédure

Sur le nœud du Gestionnaire de cellule principal, effectuez les opérations suivantes :

1. Vérifiez la présence éventuelle d'erreurs dans le fichier de configuration (par exemple, `cluster.conf`) :

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

   Si vous détectez des erreurs, corrigez-les.

   S'il n'existe aucune erreur, activez la configuration :

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

2. Démarrez le cluster, s'il n'est pas déjà en cours d'exécution :

   ```
   cmruncl
   ```

3. Créez et modifiez les fichiers de package cluster Data Protector (configuration et contrôle). Pour les packages modulaires, créez et modifiez le fichier de package de cluster simple (configuration).

   a. Créez le sous-répertoire dans le répertoire `/etc/cmcluster` qui contiendra le package Data Protector :

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

   b. Accédez au répertoire `/etc/cmcluster/ob2cl`:

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

   c. Pour les packages existants, créez un fichier de configuration de package dans le répertoire du package Data Protector :

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

      Pour les packages modulaires, utilisez la commande :

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

   d. Cette étape doit être effectuée pour les packages existants seulement. Créez un fichier de contrôle de package dans le répertoire de package Data Protector : `cmmakepkg -s /etc/cmcluster/ob2cl/ob2cl.cntl`.

   e. Modifiez le fichier de configuration de package Data Protector (par exemple, `/etc/cmcluster/ob2cl/ob2cl.conf`). Pour plus d'informations, reportez-vous à Modifier le fichier de configuration de package Data Protector, Page 174.

   f. Cette étape doit être effectuée pour les packages existants seulement. Modifiez le fichier de contrôle de package Data Protector (par exemple, `/etc/cmcluster/ob2cl/ob2cl.cntl`). Pour plus d'informations, reportez-vous à Modifier le fichier de contrôle de package Data Protector, Page 176.

4. Vérifiez et propagez les fichiers de package de cluster Data Protector.

   a. Pour les packages existants, copiez le fichier de contrôle de package sur un autre nœud, appelé `system2`, dans le cluster :

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

   b. Activez le disque partagé Data Protector en tant que groupe de volumes de cluster (créé précédemment) sur tous les nœuds de cluster :

      HP-UX :

      ```
      vgchange -c y vg_name
      ```

      Linux :

      ```
      vgchange -a y vg_name
      ```

c. Vérifiez le package Data Protector :

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

Si la vérification est correcte, ajoutez le package Data Protector :

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

d. Démarrez le package :

```
cmrunpkg ob2cl
```

Le cluster doit être formé et le package Gestionnaire de cellule Data Protector doit être opérationnel.

5. Sur le nœud principal, mettez à jour le nom d'hôte du cluster dans l'IDB et le client de domaine Data Protector du serveur d'application. Exécutez la commande suivante, une seule fois sur le premier nœud actif ::

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

Installation dans Serveur d'installation sur des nœuds cluster

Vous pouvez installer Serveur d'installation sur un nœud Serviceguard secondaire et l'utiliser pour une installation à distance. Installer des Serveur d'installation pour systèmes UNIX, Page 42.

> **REMARQUE :**
> Si vous mettez en place le serveur d'Installation avant de configurer le nœud principal en tant que gestionnaire de cellule compatible cluster, assurez-vous que le serveur d'Installation est installé sur chacun des nœuds du cluster secondaire. Le serveur d'installation est importé avec le nom du serveur virtuel lors de la configuration du nœud principal. Si le serveur d'installation n'est pas installé sur chacun des nœuds de cluster, son nom de serveur virtuel doit être exporté depuis la liste des serveurs d'installation. En outre, chacun des noms de nœuds de cluster physiquement associés doivent être importés une fois la configuration du gestionnaire de cellule compatible cluster terminée.

Installation de clients compatibles cluster

> **IMPORTANT :**
> Les clients compatibles cluster Data Protector doivent être installés sur tous les nœuds de cluster.

La procédure d'installation est la procédure standard d'installation de Data Protector sur un client UNIX. Pour obtenir des instructions détaillées, reportez-vous à Installation de clients HP-UX , Page 71 et Installation de clients Linux, Page 82.

Étapes suivantes

Lorsque l'installation est terminée, vous devez importer le serveur virtuel (le nom d'hôte spécifié dans le package cluster) sur la cellule Data Protector. Voir Importation d'un client compatible cluster vers une cellule, Page 195.

Pour plus d'informations sur la configuration de périphériques de sauvegarde, de pools de supports ou toute tâche de configuration Data Protector supplémentaire, consultez l'index *Aide de Data Protector* : "configuration".

Exemple de création de groupe de volumes

Créez un groupe de volumes sur un disque partagé accessible aux deux Gestionnaires de cellule.

> **REMARQUE :**
> Si vous utilisez le disque `ob2` comme disque de verrouillage de cluster, vous devez déjà avoir créé un groupe de volumes correspondant.

Opérations sur le nœud du Gestionnaire de cellule principal

Sur le nœud du Gestionnaire de cellule principal, effectuez les opérations suivantes :

1. a. Créez un répertoire pour un nouveau groupe de volumes :

   `mkdir vg_name`

   > **REMARQUE :**
   > `vg_name` est le chemin d'accès du groupe de volumes situé dans un sous-répertoire du répertoire `/dev`.

   b. Établissez une liste de tous les groupes de volumes existants sur le système pour vérifier les numéros mineurs qui sont utilisés :

   `ll /dev/*/group`

   c. Créez un fichier de groupe pour le groupe de volumes :

   `mknod vg_name/group c 64 0xNN0000`

   > **REMARQUE :**
   > `NN` est le numéro mineur disponible.

   d. Créez un volume physique sur le(s) disque(s) utilisé(s) pour le Gestionnaire de cellule Data Protector :

   `pvcreate -f pv_path ...`

   > **REMARQUE :**
   > `pv_path` utilisé avec la commande `pvcreate`, désigne les chemins d'accès aux périphériques caractères (raw) des volumes physiques du sous-répertoire du répertoire `/dev/rdsk` (par exemple, le `character pv_path` pour le volume physique `c0t1d0` est `/dev/rdsk/c0t1d0`).

   e. Créez un nouveau groupe de volumes :

   `vgcreate vg_name pv_path ...`

   > **REMARQUE :**
   > `pv_path` utilisé avec la commande `vgcreate` désigne le nom du chemin d'accès du

> périphérique de bloc pour le volume physique qui sera attribué au nouveau groupe de volumes. Il est situé dans un sous-répertoire du répertoire `/dev/dsk` (par exemple, le `block pv_path` pour le volume physique `c0t1d0` est `/dev/dsk/c0t1d0`).

2. Créez un volume logique pour ce groupe.
   a. Créez un nouveau volume logique pour le groupe de volumes :

      `lvcreate -L lv_size -n lv_name vg_name`

      > **REMARQUE :**
      > Les répertoires Data Protector `/etc/opt/omni` et `/var/opt/omni` sont disponibles ici.
      >
      > *`lv_size`* est le nombre représentant la taille de la partition en Mo.
      >
      > *`lv_name`* est le nom du volume logique.

   b. Créez un système de fichiers journaux sur le volume logique :

      `newfs -F FStype lv_path`

      > **REMARQUE :**
      > *`FStype`* spécifie le type de système de fichiers sur lequel opérer.
      >
      > *`lv_path`* est le nom du chemin du périphérique à caractère spécial (raw) du volume logique.

3. Définissez les propriétés du groupe de volumes en suivant la documentation du cluster.

   HP-UX :

   a. Désactivez le groupe de volumes du mode normal :

      `vgchange -a n vg_name`

   b. Marquez le groupe de volumes pour l'utilisation du cluster :

      `vgchange -c y vg_name`

      > **REMARQUE :**
      > s'il s'agit d'un disque de verrouillage de cluster et si vous utilisez une version ultérieure de Serviceguard (par exemple, 11.09), l'opération est effectuée automatiquement.

   c. Utilisez le groupe de volumes en mode exclusif :

      `vgchange -a e vg_name`

   Linux :

   a. Désactivez le groupe de volumes du mode normal :

      `vgchange -a n vg_name`

   b. Marquez le groupe de volumes pour l'utilisation du cluster :

      `vgchange -a y vg_name`

4. Créez un répertoire de point de montage (par exemple, `/omni_shared`), puis montez le volume logique dans ce répertoire :
   a. `mkdir shared_dirname`
   b. `mount lv_path shared_dirname`
5. Démontez le répertoire du point de montage :

```
umount shared_dirname
```

6. Désactivez le groupe de volumes que vous avez créé :

   ```
   vgchange -a n vg_name
   ```

7. Exportez le groupe de volumes que vous avez créé sur le Gestionnaire de cellule principal.
   a. Exportez les informations de configuration LVM à partir de system1 :

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

      > **REMARQUE :**
      > *mapfile* spécifie ici le chemin du fichier dans lequel les noms et numéros des volumes logiques seront écrits.

   b. Transférez le fichier map sur system2 :

      ```
      rcp mapfile second_system: mapfile
      ```

Opérations sur le nœud du Gestionnaire de cellule secondaire

Sur le nœud du Gestionnaire de cellule secondaire, effectuez les opérations suivantes :

1. Créez le groupe de volumes à importer, et importez-le.
   a. Créez un répertoire pour un nouveau groupe de volumes :

      ```
      mkdir vg_name
      ```

      > **REMARQUE :**
      > *vg_name* est le chemin d'accès du groupe de volumes situé dans un sous-répertoire du répertoire `/dev`.

   b. Établissez une liste de tous les groupes de volumes existants sur le système pour vérifier les numéros mineurs qui sont utilisés :

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

   c. Créez un fichier de groupe pour le groupe de volumes :

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

      > **REMARQUE :**
      > `NN` est le numéro mineur disponible.

   d. Importez le groupe de volumes :

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

      > **REMARQUE :**
      > *mapfile* représente le chemin du fichier à partir duquel les noms et numéros des volumes logiques seront lus.
      >
      > *pv_path* est le nom du chemin du périphérique de blocs du volume physique.

2. Définissez les propriétés du groupe de volumes.

   HP-UX :

a. Désactivez le groupe de volumes du mode normal :

```
vgchange -a n vg_name
```

b. Marquez le groupe de volumes pour l'utilisation du cluster :

```
vgchange -c y vg_name
```

> **REMARQUE :**
> s'il s'agit d'un disque de verrouillage de cluster et si vous utilisez une version ultérieure de Serviceguard (par exemple, 11.09), l'opération est effectuée automatiquement.

c. Utilisez le groupe de volumes en mode exclusif :

```
vgchange -a e vg_name
```

Linux :

a. Désactivez le groupe de volumes du mode normal :

```
vgchange -a n vg_name
```

b. Marquez le groupe de volumes pour l'utilisation du cluster :

```
vgchange -a y vg_name
```

3. Créez le même répertoire de point de montage que celui créé sur le Gestionnaire de cellule principal, puis montez le volume logique dans ce répertoire.
4. Démontez le répertoire du point de montage :

```
umount shared_dirname
```

5. Désactivez le groupe de volumes que vous avez importé :

```
vgchange -a n vg_name
```

Modifier le fichier de configuration de package Data Protector

Dans le fichier de configuration de package modulaire Data Protector, modifiez les champs suivants :

Par exemple :

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

Les paramètres de sous-réseau sont les suivants :

Par exemple :

monitored_subnet	10.81.0.0
ip_subnet	10.81.0.0
ip_address	10.81.8.46

REMARQUE :
`monitored_subnet` est le sous-réseau qui comprend les nœuds de clusters.

`ip_subnet` est le sous-réseau qui comprend l'IP du serveur virtuel du gestionnaire de cellule Data Protector.

`ip_address` est l'IP du serveur virtuel du gestionnaire de cellule Data Protector

Les paramètres de services Data Protector sont les suivants :

Par exemple :

`service_name`	`dp_svc`
`service_cmd`	`/opt/omni/sbin/csfailover.ksh start`
`service_restart`	`None`
`service_fail_fast_enabled`	`no`
`service_halt_timeout`	`300`

REMARQUE :
Le `service_cmd` doit être configuré sur `/opt/omni/sbin/csfailover.ksh start`.

Les informations de systèmes de fichiers partagés Data Protector sont les suivantes :

Par exemple :

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

Dans le fichier de configuration de package existant Data Protector, modifiez les champs suivants :

`PACKAGE_NAME`

`NODE_NAME`

`RUN_SCRIPT` (il s'agit du même fichier que le fichier de contrôle du package Data Protector).

`HALT_SCRIPT` (il s'agit du même fichier que le fichier de contrôle du package Data Protector).

`MONITORED_SUBNET`

`SERVICE_NAME` (vous pouvez saisir le nom que vous voulez, mais vous devez utiliser le même nom dans le fichier de contrôle.)

`SERVICE_FAIL_FAST_ENABLED`

SERVICE_HALT_TIMEOUT

Par exemple :

PACKAGE_NAME	ob2cl
NODE_NAME	onca
NODE_NAME	pardus
RUN_SCRIPT	/etc/cmcluster/ob2cl/ob2cl.cntl
HALT_SCRIPT	/etc/cmcluster/ob2cl/ob2cl.cntl
MONITORED_SUBNET	10.17.0.0
SERVICE_NAME	omni_sv
SERVICE_FAIL_FAST_ENABLED	NO
SERVICE_HALT_TIMEOUT	300

Modifier le fichier de contrôle de package Data Protector

Dans le fichier de contrôle de package existant Data Protector, modifiez les champs suivants :

VG [n]

LV [n]

FS [n]

FS_MOUNT_OPT [n]

IP

SUBNET

SERVICE_NAME (le même que celui utilisé dans le fichier de configuration)

SERVICE_CMD (Doit être: /opt/omni/sbin/csfailover.ksh start)

Par exemple :

VG[0]	vg_dp
LV[0]	/dev/vg_dp/dp_share
FS[0]	/DP_SHARE
FS_MOUNT_OPT[0]	-o rw
FS_TYPE[0]	vxfs
IP[0]	10.17.17.69
SUBNET[0]	10.17.0.0

SERVICE_NAME[0]	omni_sv
SERVICE_CMD[0]	/opt/omni/sbin/csfailover.ksh start

Installation de Data Protector sur Symantec Veritas Cluster Server

Data Protector prend en charge Symantec Veritas Cluster Server (VCS) pour Linux. Pour connaître les versions des systèmes d'exploitation pris en charge, consultez la dernière *Data Protector Matrice de prise en charge de la plate-forme et de l'intégration*.

> **REMARQUE :**
> Si vous avez configuré l'IP de groupe de services Data Protector, utilisez cette IP pour l'octroi de licence. Si vous avez configuré le groupe de services Data Protector sans l'adresse IP, utilisez l'IP Veritas Cluster pour l'octroi de licence.

Etapes de la configuration

1. Configuration du Gestionnaire de cellule principal
2. Configuration du Gestionnaire de cellule secondaire
3. Configuration du groupe services de cluster pour le Gestionnaire de cellule

Installation d'un Gestionnaire de cellule compatible cluster

Conditions préalables

Avant d'installer un Data Protector Gestionnaire de cellule sur VCS, vérifiez ce qui suit :

- Identifiez le ou les systèmes principaux et secondaires Gestionnaire de cellule. Tous doivent disposer de Symantec Veritas Cluster Server et doivent être configurés en tant que membres de cluster.
- Vous devez installer le Data Protector Gestionnaire de cellule, avec les correctifs et tous les autres composants logiciels Data Protector recommandés pour les intégrations voulues dans le cluster, sur le nœud principal et sur chacun des nœuds secondaires.
- Le groupe d'utilisateurs hpdp et le compte utilisateur dédié hpdp doivent avoir les mêmes ID sur les deux nœuds.
- Dans cet environnement de cluster, un Data Protector Gestionnaire de cellule doit avoir son propre groupe de services de cluster, qui doit être créé et préparé avant la configuration Gestionnaire de cellule configuration de cluster. Avant d'installer le Data Protector Gestionnaire de cellule dans VCS, vous devez obtenir le nom de serveur virtuel et son adresse IP correspondante. Cette adresse IP ou nom de serveur est par la suite utilisé comme nom de serveur virtuel Data Protector

Gestionnaire de cellule ou adresse IP de groupe de services Data Protector.

- Vérifiez que les noeuds cluster et l'adresse IP (virtuelle) du groupe de services Data Protector figurent dans le même sous-réseau.

  > **REMARQUE :**
  > Vérifiez que l'adresse IP du groupe de services Data Protector et celle de Veritas Cluster sont différentes.

- Si vous disposez du service DNS dans votre environnement, vérifiez que tous les nœuds dans le cluster, ainsi que l'adresse IP du groupe de services Data Protector sont enregistrés auprès du serveur DNS.
- Lorsque l'installation est terminée, vous devez configurer le Gestionnaire de cellule principal installé, le ou les Gestionnaires de cellule secondaires et le package du Gestionnaire de cellule.

Préparation du groupe de services de cluster pour Data Protector Gestionnaire de cellule

Vous devez créer un groupe de services (Data Protector) de cluster avec les ressources suivantes :

- Ressource de cluster IP - Se réfère à l'adresse IP virtuelle utilisée pour la configuration de ressource IP.
- Ressource de cluster de montage - Se réfère à la ressource de montage avec les ressources dépendantes correspondantes pour contrôler le volume partagé créé sur un disque partagé et accessible depuis tous les nœuds, où Data Protector pourrait être en cours d'exécution. Ce volume partagé est utilisé pour les fichiers de configuration et de données Data Protector parmi les nœuds.

Configuring the Primary Gestionnaire de cellule

Procédure

1. Démarrez le groupe de services Data Protector sur le nœud principal.
2. Modifiez le fichier de modèle `/etc/opt/omni/server/sg/sg.conf`.

   > **REMARQUE :**
   > L'option `SHARED_DISK_ROOT` doit contenir le nom de votre répertoire de point de montage (par exemple, `SHARED DISK ROOT=/omni_shared`).
   >
   > L'option `CS_SERVICE_HOSTNAME` doit contenir le nom du Gestionnaire de cellule virtuel, tel qu'il est connu sur le réseau. (Par exemple, `CS_SERVICE HOSTNAME=dpvcs.company.com`.)

3. Configurez le Gestionnaire de cellule principal. Assurez-vous que le script n'est pas exécuté depuis les répertoires `/etc/opt/omni/` ou `/var/opt/omni/`, ni l'un de leurs sous-répertoires. Assurez-vous également qu'aucun sous-répertoire n'est monté dans le répertoire `/etc/opt/omni/` ou `/var/opt/omni/`. Exécutez la commande suivante :

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

   > **REMARQUE :**
   > Après l'exécution de ce script, les services Data Protector sont arrêtés et seront

redémarrés ultérieurement.

Configuration du Gestionnaire de cellule secondaire

Procédure

1. Faites basculer le groupe de services Data Protector sur le nœud secondaire.
2. Configurez le Gestionnaire de cellule secondaire :

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

   où *`dirname`* est le point de montage ou répertoire partagé (par exemple, `/omni_shared`).

Configuration du groupe services de cluster pour le Gestionnaire de cellule

Procédure

1. Faites basculer le groupe de services Data Protector sur le nœud principal.
2. Ajoutez la ressource d'application de cluster, qui sera utilisée pour surveiller et contrôler les services Data Protector du groupe de services Data Protector et utilisez le script `vcsfailover.ksh` comme moniteur d'application ou programme de contrôle. Par exemple,

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

   REMARQUE :
   Si le script `vcsfailover.ksh` doit être personnalisé, une copie de ce script doit être créée et utilisée comme moniteur ou programme de contrôle. Pendant les mises à niveau ou à jour, le script d'origine est écrasé et le script personnalisé doit être manuellement mis à jour avec les nouvelles modifications (le cas échéant).
3. Créez la ressource d'application Data Protector.

   REMARQUE :
   Rendez la ressource d'application Data Protector dépendante des ressources de montage et IP de serveur virtuel.
4. Activez et démarrez la ressource d'application Data Protector.

Installation dans Serveur d'installation sur des nœuds cluster

Vous pouvez installer Serveur d'installation sur un nœud Symantec Veritas Cluster Server secondaire et l'utilise pour une installation à distance. Installer des Serveur d'installation pour systèmes UNIX, Page 42.

> **REMARQUE :**
> Si vous mettez en place le serveur d'Installation avant de configurer le nœud principal en tant que gestionnaire de cellule compatible cluster, assurez-vous que le serveur d'Installation est installé sur chacun des nœuds du cluster secondaire. Le serveur d'installation est importé avec le nom du serveur virtuel lors de la configuration du nœud principal. Si le serveur d'installation n'est pas installé sur chacun des nœuds de cluster, son nom de serveur virtuel doit être exporté depuis la liste des serveurs d'installation. En outre, chacun des noms de nœuds de cluster physiquement associés doivent être importés une fois la configuration du gestionnaire de cellule compatible cluster terminée.

Installation de clients compatibles cluster

La procédure d'installation est la procédure standard d'installation de Data Protector sur un système client. Pour des instructions détaillées, reportez-vous à la section Installer des clients Data Protector, Page 54.

Étapes suivantes

Lorsque l'installation est terminée :

- Pour sauvegarder le serveur virtuel, vous devez l'importer dans la cellule.
- Pour sauvegarder les nœuds physiques, vous devez aussi les importer dans la cellule.

Voir Importation d'un client compatible cluster vers une cellule, Page 195. Pour plus d'informations sur la configuration de périphériques de sauvegarde, de pools de supports ou toute tâche de configuration Data Protector supplémentaire, consultez l'index *Aide de Data Protector* : "Configuration".

Installation de Data Protector sur Microsoft Cluster Server

Pour connaître les systèmes d'exploitation prix en charge pour l'intégration de Microsoft Cluster Server, consultez les dernières matrices de prise en charge sur https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.

> **REMARQUE :**
> Si votre Gestionnaire de cellule doit être compatible cluster, l'adresse IP du serveur virtuel Gestionnaire de cellule doit être utilisée pour les licences.

Installation d'un Gestionnaire de cellule compatible cluster

Conditions préalables

Pour que vous puissiez installer le Data Protector Gestionnaire de cellule compatible cluster, les conditions préalables suivantes doivent être remplies :

- La fonctionnalité de cluster doit être installée sur tous les nœuds cluster. Par exemple, vous devez pouvoir déplacer des groupes d'un nœud à l'autre autant de fois que cela est nécessaire, et ce sans aucun problème de disque partagé.
- Veillez à ce qu'il n'existe pas sur le cluster de ressources avec les noms suivants :

  `OBVS_MCRS`, `OBVS_HPDP_AS`, `OBVS_HPDP_IDB`, `OBVS_HPDP_IDB_CP` et `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 :

  1. Cliquez sur **Démarrer** > **Programmes** >**Outils administratifs** > **Administrateur de clusters**.
  2. Vérifiez la liste des ressources et supprimez ou renommez ces ressources, si nécessaire.
- Au moins un groupe du cluster doit contenir 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.

  Windows Server 2008, Windows Server 2012 : les fichiers de données sont installés dans le dossier partagé de la ressource *Serveur de fichiers* sélectionné par l'utilisateur lors de l'installation.

  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`.
- Soit le serveur virtuel n'existe pas dans le même groupe en tant que ressource de cluster de fichiers, soit vous devez créer un serveur virtuel en utilisant une adresse IP libre enregistrée et lui associer un nom de réseau.
- La ressource de cluster de fichiers dans laquelle Data Protector sera installé doit disposer d'une `IP Address`, d'un `Network Name` et d'un `Physical Disk` définis parmi ses dépendances. Cela permet l'exécution du groupe de clusters Data Protector sur n'importe quel nœud, indépendamment de tout autre groupe.
- Vérifiez que seul l'administrateur de clusters a accès au dossier partagé de la ressource de cluster de fichiers et qu'il dispose d'un accès complet.
- Data Protector est installé au même emplacement (lecteur et chemin d'accès) sur tous les nœuds cluster. Assurez-vous que ces emplacements sont libres.
- Si vous démarrez l'installation du Gestionnaire de cellule compatible cluster à partir d'un partage de réseau, vous devez pouvoir accéder à ce partage à partir de tous les nœuds 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 (nœud) du cluster doit être en cours d'exécution.
- Pour activer l'installation d'un client Data Protector Gestionnaire de cellule compatible cluster sur un cluster de serveurs avec Microsoft Cluster Service (MSCS) exécuté sur Windows Server 2008 ou Windows Server 2012, effectuez la procédure décrite dans Préparation d'une grappe de serveurs Microsoft sous Windows Server 2008 ou Windows Server 2012 pour une installation de Data Protector, Page 356.

Points à prendre en considération

- L'installation doit être démarrée sous le compte de service cluster sur le système (nœud) sur lequel la ressource de cluster de fichiers est active, afin de permettre un accès direct à son dossier partagé. 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 Data ProtectorGestionnaire de cellule compatible cluster, un compte de domaine avec les droits d'utilisateur suivants doit être fourni pendant l'installation :
  - Droits administrateur sur le système du 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 doté de droits d'administrateur sur tous les systèmes de clusters (nœuds). Vous devez également utiliser ce compte pour installer Data Protector. Sinon, les services Data Protector s'exécutent en mode ordinaire au lieu du mode compatible cluster.
- Le compte utilisateur du domaine Windows utilisé par le service Inet doit de plus obtenir les privilèges de stratégie de sécurité du système d'exploitation Windows sur tous les nœuds du cluster :
  - Emprunter l'identité d'un client après l'authentification
  - Remplacer un jeton de niveau processus

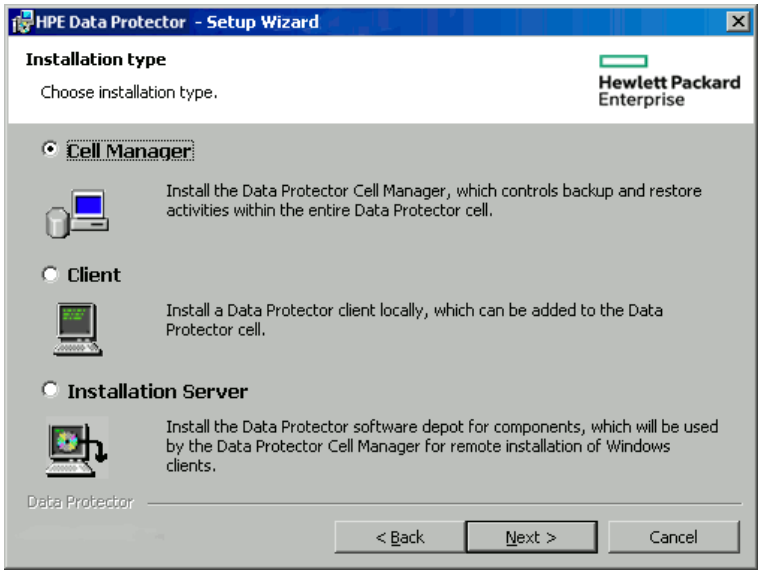
  Reportez-vous à l'index *Aide de Data Protector* : "Emprunt d'identité d'utilisateur Inet".

Procédure d'installation locale

Le Data Protector Gestionnaire de cellule compatible cluster doit être installé localement, à partir du package d'installation. Effectuez les opérations suivantes :

1. Copiez le package d'installation téléchargé (zip) sur un système Windows et décompressez les fichiers dans un répertoire local. Exécute le fichier `setup.exe` à partir du dossier correspondant à votre plate-forme.
2. Suivez les instructions de l'assistant et lisez attentivement le contrat de licence. Si vous en acceptez les conditions du contrat, cliquez sur **Suivant** pour continuer.
3. Examinez les détails de la page Informations d'obsolescence et cliquez sur **Je comprends les changements apportés aux plates-formes prises en charges**, uniquement si vous acceptez modifications apportées par Data Protector à la liste des versions logicielles et matérielles prises en charge.
4. Sur la page Type d'installation, sélectionnez **Gestionnaire de cellule**, puis cliquez sur **Suivant** pour installer le logiciel Data Protector Gestionnaire de cellule.

   Sélectionner le type d'installation

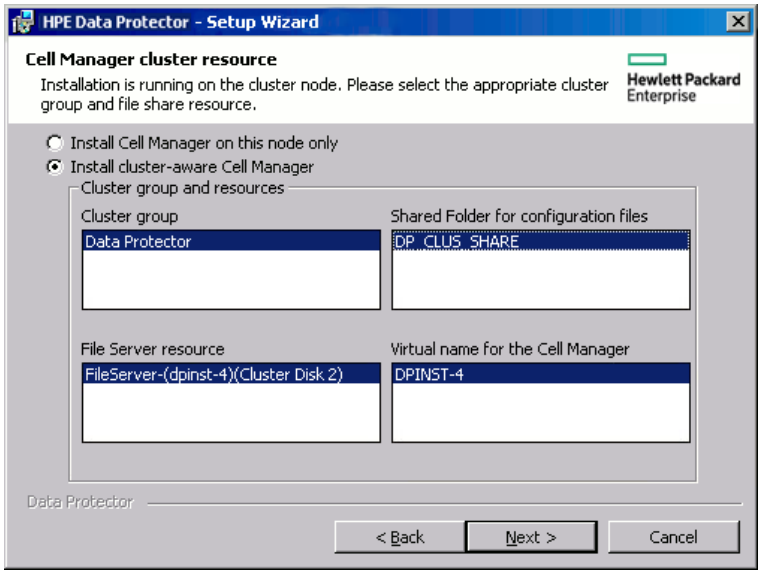


5. Le processus d'installation détecte automatiquement qu'il fonctionne dans un environnement de clusters. Sélectionnez **Installer le Gestionnaire de cellule compatible cluster** pour activer une configuration en cluster.

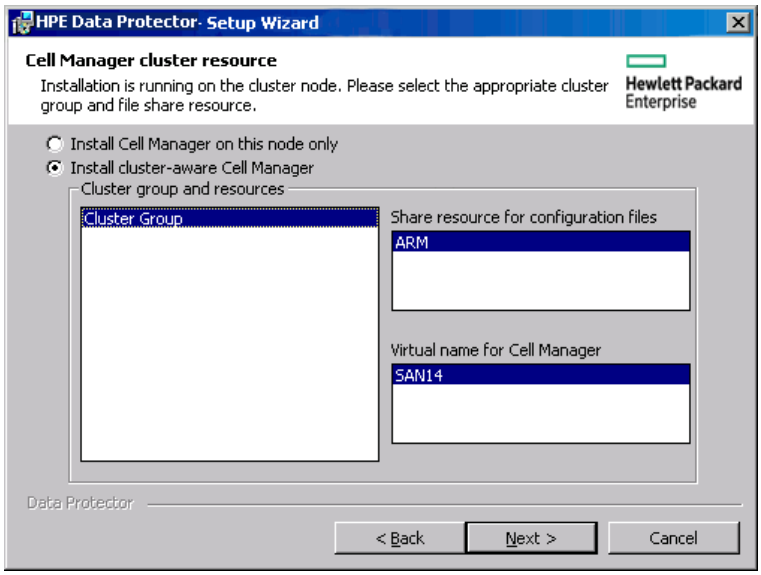
   Sélectionnez le groupe de clusters, le nom d'hôte virtuel et la ressource de cluster de fichiers sur laquelle résideront les fichiers partagés et la base de données de Data Protector.

   > **REMARQUE :**
   > si vous sélectionnez **Installer le Gestionnaire de cellule sur ce nœud uniquement**, le Gestionnaire de cellule se sera *pas* compatible cluster. Voir Installing a Windows Gestionnaire de cellule, Page 34.

   Sélection de la ressource de cluster sur Windows Server 2008

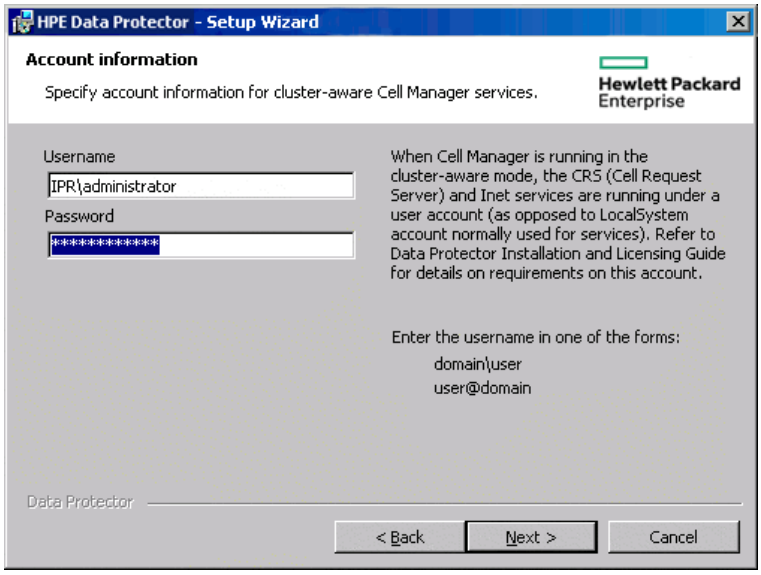


Sélection de la ressource de cluster sur les autres systèmes Windows



6. Saisissez le nom d'utilisateur et le mot de passe correspondant au compte qui sera utilisé pour lancer les services Data Protector.

   Insertion des informations du compte



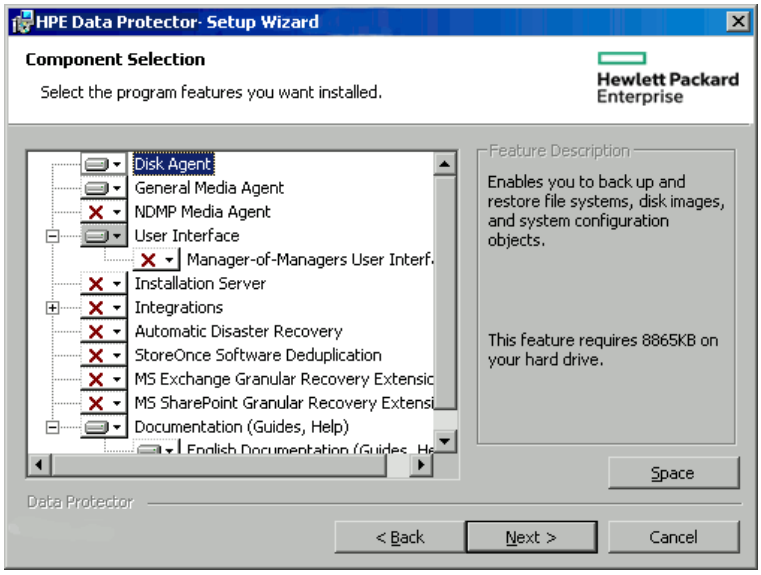
7. Cliquez sur **Suivant** pour installer Data Protector dans les dossiers d'installation par défaut.

   Sinon, cliquez sur **Changer** pour ouvrir la boîte de dialogue Changer le dossier de destination actuel ou Changer le dossier de destination des données du programme actuel, et changez le dossier d'installation comme requis. Le chemin vers le dossier d'installation des données du programme ne doit pas dépasser 80 caractères.
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 Pris en charge du cluster MS sont installés automatiquement.

   Les composants sélectionnés seront installés sur tous les nœuds cluster.

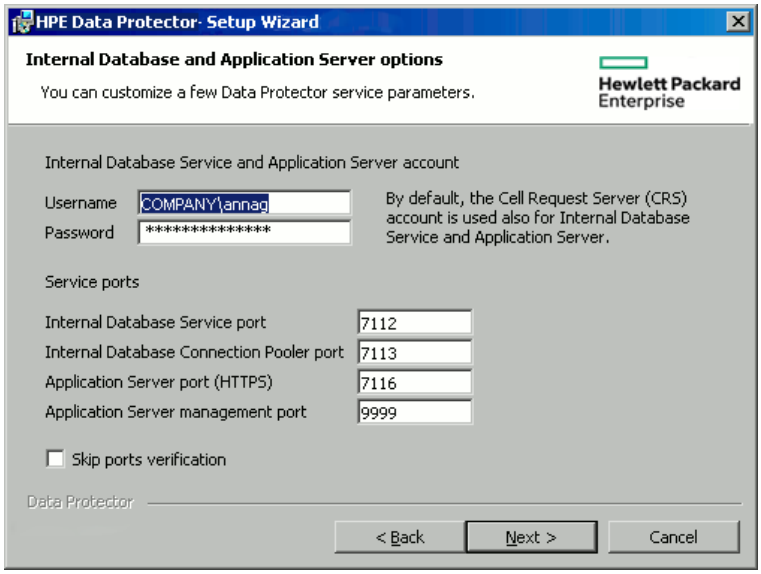
   Page de sélection de composant



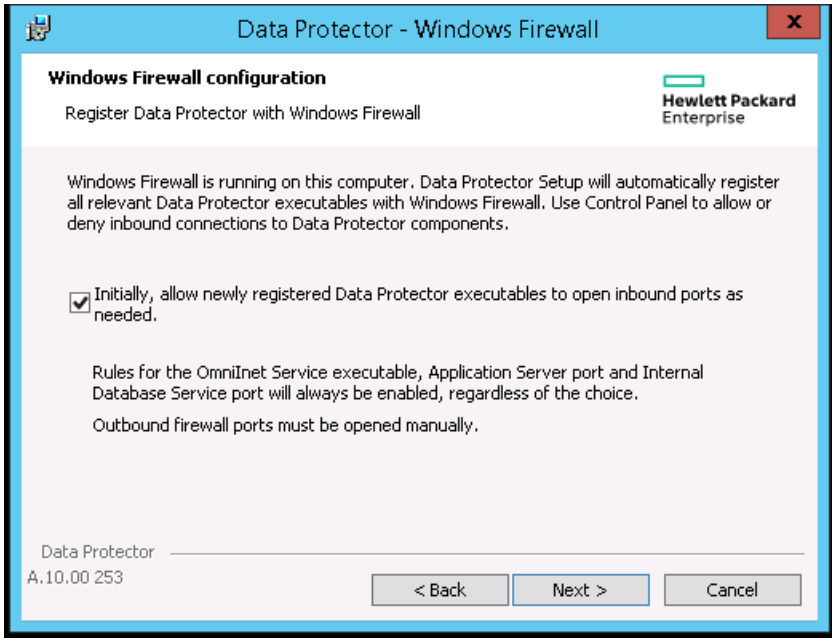
9. Vous pouvez, si vous le souhaitez, modifier le compteur utilisateur ou les ports utilisés par le service de Base de données interne et le serveur d'application des services Data Protector.

Cliquez sur **Suivant**.

Changer les options d'IDB et de Serveur d'application



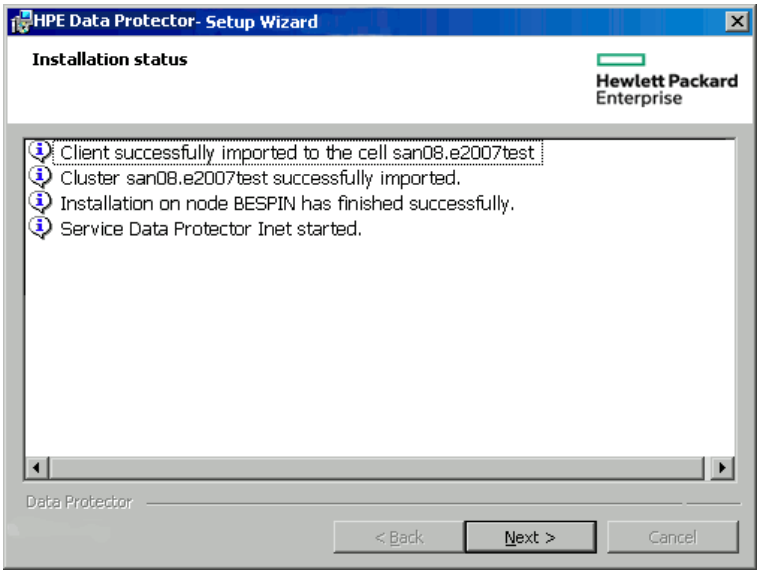
10. Si Data Protector détecte Windows Firewall sur votre système, la page de configuration de Windows Firewall s'affiche. Le processus de configuration de Data Protector enregistre tous les exécutables Data Protector. Par défaut, l'option **Permettre initialement aux nouveaux fichiers binaires Data Protector enregistrés d'ouvrir des ports le cas échéant** est sélectionnée. Si vous ne souhaitez pas permettre à Data Protector d'ouvrir les ports pour le moment, ne cochez pas l'option. Pour un fonctionnement correct de Data Protector avec la version précédente des clients 10.00, les règles Data Protector dans le pare-feu Windows doivent être activées. Les règles pour l'exécutable du service OmniInet, le port du serveur d'application et le port de l'IDS seront toujours activées, indépendamment du choix effectué.



Cliquez sur **Suivant**.

11. La liste des composants sélectionnés s'affiche. Cliquez sur **Installer**.
12. La page de configuration de l'installation s'ouvre. Cliquez sur **Suivant**.

    Page État de l'installation



13. Si vous avez installé le composant `User Interface`, pour commencer à utiliser l'interface utilisateur graphique Data Protector immédiatement après l'installation, sélectionnez, sélectionnez **Lancer l'interface utilisateur graphique de Data Protector**.

    Si vous avez installé le composant `English Documentation (Guides, Help)`, pour voir les Annonces sur les produits, notes sur les logiciels et références Data Protector immédiatement après l'installation, sélectionnez **Références, notes de publication et annonces produits**.
14. Cliquez sur **Terminer** pour terminer l'installation.

Installation d'un Gestionnaire de cellule compatible cluster pour les clusters Windows 2012 et Windows 2012 R2

Pour installer un Gestionnaire de cellule compatible cluster

1. Installez le Serveur d'installation Data Protector sur une machine ne faisant pas partie du cluster.
2. Appliquez le dernier correctif sur celui-ci. Le dépôt dans `'\DP_Program_data\Depot'` du Serveur d'installation peut être utilisé pour installer le Gestionnaire de cellule compatible cluster dans les systèmes Windows 2012 et 2012 R2.
3. Copiez le dépôt vers l'un des nœuds cluster et démarrez l'installation à partir du disque local.
4. Vous avez également la possibilité d'accéder au dépôt à l'aide d'un partage réseau et de démarrer l'installation à partir du partage. Pour cette étape, vous devez également tenir compte des points suivants :
   - Le serveur d'installation doit se trouver dans le même domaine que le cluster.
   - Les partages administratifs (masqués) (`\\hostname or IP address of IS\c$\...`) ne doivent pas être utilisés. En effet, dans certains cas, il ne sera pas possible d'y accéder à partir d'autres nœuds cluster. Par conséquent, les chemins d'accès normaux (`\\hostname or IP address of IS\depot`) doivent être utilisés et partagés avec tous les nœuds cluster.

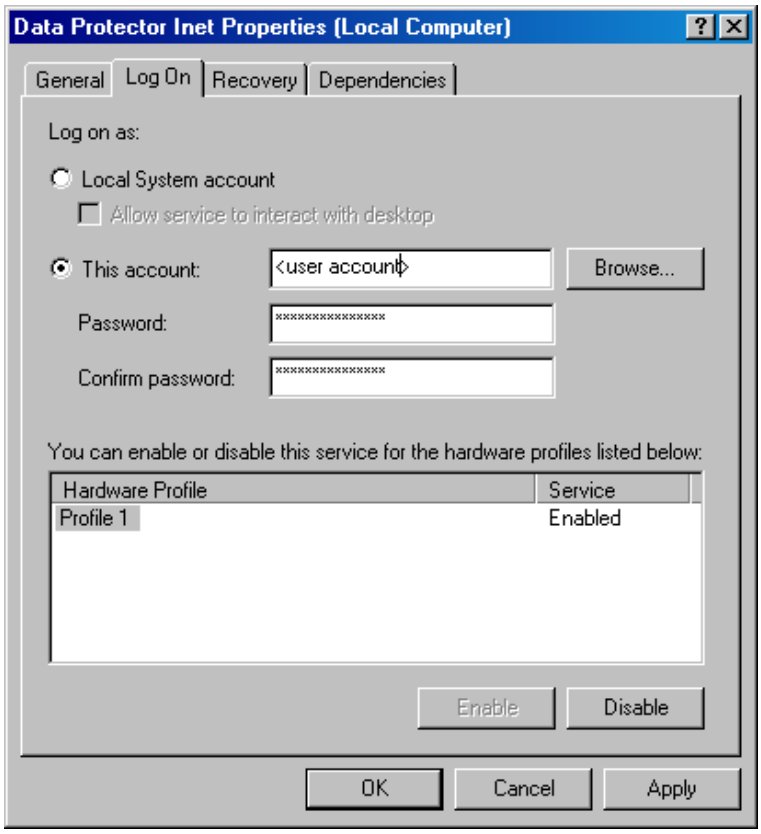
- Les nœuds cluster doivent avoir la possibilité de se connecter au chemin d'accès net normal sans utiliser de mot de passe.
- Le chemin d'accès net normal doit être accessible à partir d'un navigateur sans fournir d'informations d'identification. Si on vous demande des informations d'identification, saisissez-les et sélectionnez Mémoriser mes identifiants.

Vérification de l'installation

Lorsque la procédure de configuration est terminée, vous pouvez vérifier si le logiciel Data Protector a été correctement installé. Procédez comme suit :

1. Vérifiez si le compte de service Cluster est attribué au service Data Protector `Inet` sur chaque nœud du cluster. Assurez-vous que le même utilisateur est également ajouté au Groupe d'utilisateurs Admin de Data Protector. Le type de compte de connexion doit être défini sur `This account`, comme indiqué dans Compte utilisateur Data Protector, bas.

   Compte utilisateur Data Protector

2. Exécuter la commande suivante :

   `omnirsh` *`host`* `INFO_CLUS`

   avec *host* étant le nom du serveur virtuel de cluster (respect de la casse). Le résultat doit contenir les noms des systèmes 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. Démarrez l'interface graphique Data Protector, sélectionnez le contexte de **Clients**, puis cliquez

sur **MS Clusters.** Reportez-vous aux nouveaux systèmes installés, répertoriés dans la zone de résultats.

Services Inet et CRS Data Protector

Si nécessaire, modifiez les comptes sous lesquels s'exécutent les services Data Protector `Inet` et `CRS`.

Installation de clients compatibles cluster

Conditions préalables

Pour que vous puissiez installer le client Data Protector compatible cluster, les conditions préalables suivantes doivent être remplies :

- La fonctionnalité de cluster doit être installée sur tous les nœuds cluster. Par exemple, vous devez pouvoir déplacer des groupes d'un nœud à l'autre autant de fois que cela est nécessaire, et ce sans aucun problème de disque partagé.
- Chaque système du cluster doit être en cours d'exécution.
- Pour activer l'installation d'un client Data Protector compatible cluster sur un cluster de serveurs avec Microsoft Cluster Service (MSCS) exécuté sur Windows Server 2008 ou Windows Server 2012, effectuez la procédure décrite dans Préparation d'une grappe de serveurs Microsoft sous Windows Server 2008 ou Windows Server 2012 pour une installation de Data Protector, Page 356.

Procédure d'installation locale

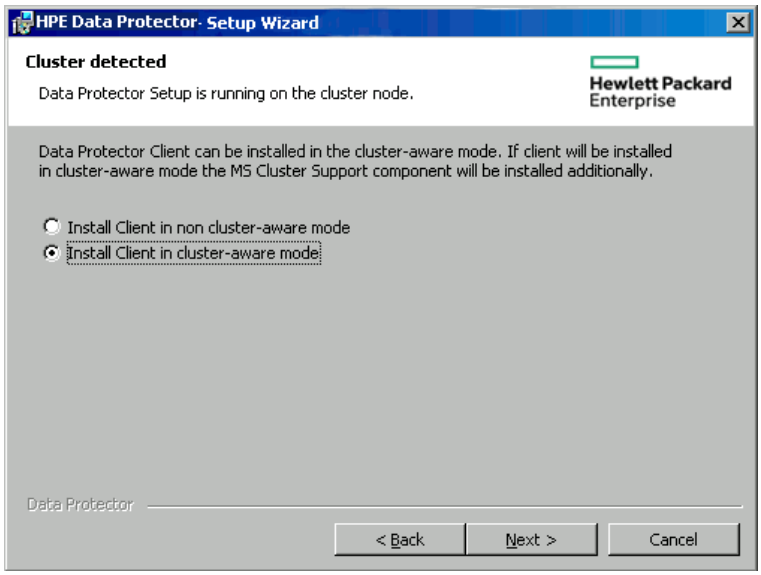
Les clients Data Protector compatibles cluster doivent être installés localement, à partir du package d'installation, sur chaque nœud cluster. Les nœuds cluster (clients cluster Data Protector) sont importés vers la cellule spécifiée lors du processus d'installation. Vous devez ensuite importer le nom du serveur virtuel.

Le compte Administrateur de cluster est requis pour effectuer l'installation. Mis à part cela, la configuration du client de cluster est identique à celle du client Windows ordinaire. Les fichiers du composant Pris en charge du cluster MS sont installés automatiquement.

Pour plus d'informations sur l'installation locale d'un système client Windows Data Protector, consultez Installation de clients Windows, Page 62.

L'installation de Data Protector rapporte qu'un cluster a été détecté. Sélectionnez **Installer le client en mode compatible cluster**.

Sélection du mode d'installation compatible cluster



Si vous installez l'intégration Oracle Data Protector, la procédure de configuration doit être réalisée sur tous les nœuds cluster et sur le serveur virtuel du groupe de ressources Oracle.

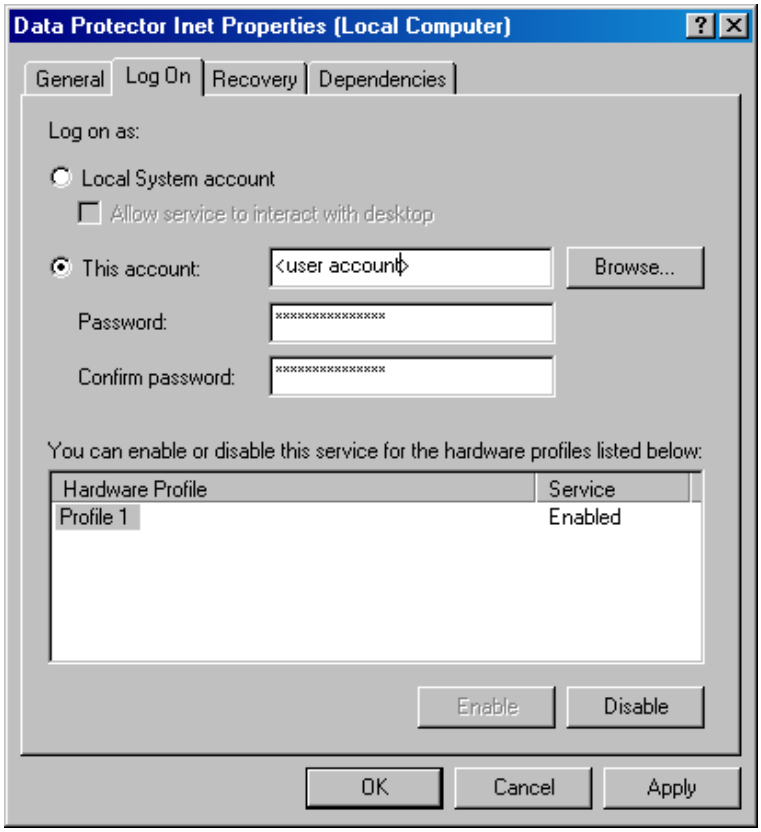
> **REMARQUE :**
> vous pouvez importer un client compatible cluster vers la cellule Data Protector qui est gérée à l'aide du Gestionnaire de cellule standard ou du Gestionnaire de cellule compatible cluster.

Vérification de l'installation

Lorsque la procédure de configuration est terminée, vous pouvez vérifier si le logiciel Data Protector a été correctement installé. Procédez comme suit :

1. Vérifiez si le compte de service Cluster est attribué au service Data Protector `Inet` sur chaque nœud du cluster. Assurez-vous que le même utilisateur est également ajouté au Groupe d'utilisateurs `admin` de Data Protector. Le type de compte de connexion doit être défini sur **Ce compte** comme indiqué dans Compte utilisateur Data Protector, bas.

   Compte utilisateur Data Protector



2. Exécutez :

   `omnirsh` *host* `INFO_CLUS`

   avec *host* étant le nom du système de client cluster. Le résultat doit contenir le nom du système client compatible cluster. Si `0 "NONE"` est affiché, Data Protector n'est pas installé en mode compatible cluster.

Gestionnaire de volume Veritas

Si Veritas Volume Manager est installé sur le cluster, des étapes supplémentaires sont nécessaires après avoir terminé l'installation de Data Protector sur le Microsoft Cluster Server. Pour les autres étapes à effectuer, voir Installation de Data Protector sur Microsoft Cluster Server avec Veritas Volume Manager, Page 358.

Étapes suivantes

Lorsque l'installation est terminée, vous devez importer le nom d'hôte du serveur virtuel (application compatible cluster) sur la cellule Data Protector. Voir Importation d'un client compatible cluster vers une cellule, Page 195.

Pour plus d'informations sur la configuration de périphériques de sauvegarde, de pools de supports ou toute tâche de configuration Data Protector supplémentaire, consultez l'index *Aide de Data Protector* : "configuration".

Modification des comptes Inet et CRS.

Si nécessaire, modifiez les comptes sous lesquels s'exécutent les services Data Protector `Inet` et `CRS`.

Installation de Data Protector sur un cluster IBM HACMP

Data Protector prend en charge l'environnement IBM HACMP (High Availability Cluster Multi-Processing) sous AIX.

> **IMPORTANT :**
> Installez le composant Data Protector Agent de disque sur tous les nœuds du cluster.

Installation de clients compatibles cluster

Pour installer les composants Data Protector sur un nœud cluster, utilisez la procédure standard d'installation de Data Protector sur les systèmes UNIX. Pour plus d'informations, voir Installation à distance, Page 95 ou Installation locale sur les systèmes UNIX et Mac OS X, Page 103.

Étapes suivantes

Après l'installation, importez les nœuds cluster et le serveur virtuel (adresse IP du package d'environnement virtuel) vers la cellule Data Protector. Voir Importation d'un client compatible cluster vers une cellule, Page 195.

Pour plus d'informations sur la configuration de périphériques de sauvegarde, de pools de supports ou toute tâche de configuration Data Protector supplémentaire, consultez l'index *Aide de Data Protector* : "configuration".

Installation de Data Protector sur un cluster Microsoft Hyper-V

L'installation de Data Protector sur des systèmes Microsoft Hyper-V qui sont configurés dans un cluster à l'aide de la fonctionnalité Microsoft Failover Clustering est similaire à l'installation de Data Protector sur Microsoft Cluster Server. Les systèmes Microsoft Hyper-V doivent devenir des clients compatibles clients Data Protector. Pour plus d'informations, voir Installation de Data Protector sur Microsoft Cluster Server, Page 180.

> **REMARQUE :**
> Lorsque les systèmes Microsoft Hyper-V deviennent des clients compatibles clusters, vous pouvez y installer à distance des composants Data Protector additionnels, à l'aide du serveur d'installation Data Protector.

Chapitre 6: Maintien de l'installation

Ce chapitre décrit les procédures les plus couramment effectuées pour modifier la configuration de votre environnement de sauvegarde. Les sections suivantes fournissent des informations sur :

- Comment et quand utiliser le mode de maintenance
- Comment importer les clients vers une cellule à l'aide de l'interface utilisateur graphique
- Comment importer un Serveur d'installation vers une cellule à l'aide de l'interface utilisateur graphique
- Comment importer les clusters/serveurs virtuels vers une cellule à l'aide de l'interface utilisateur graphique
- Comment exporter les clients à l'aide de l'interface utilisateur graphique
- Comment garantir la sécurité à l'aide de l'interface utilisateur graphique
- Comment configurer LDAP pour l'authentification d'utilisateur dans Data Protector
- Comment et quand utiliser l'utilitaire de création de certificats
- Comment gérer les paquets de correctifs Data Protector et identifier les correctifs Data Protector installés
- Comment désinstaller le logiciel Data Protector
- Comment ajouter ou supprimer des composants logiciels Data Protector

Mode maintenance Data Protector

Les tâches de maintenance sur Gestionnaire de cellule, durant lesquelles les opérations d'écriture sur la base de données interne doivent être évitées, requièrent que Data Protector entre en mode maintenance. De telles tâches incluent la mise à niveau de l'installation Data Protector, l'installation de correctifs critiques, la mise à niveau du matériel ou du système d'exploitation. Le mode maintenance est requis uniquement pour certaines procédures décrites dans ce chapitre, mais peut être appliqué également aux tâches décrites ailleurs dans cette documentation.

Le processus d'entrée en mode maintenance démarre automatiquement une série de tâches, notamment l'arrêt du planificateur, l'attribution d'un nouveau nom pour les répertoires de spécification de sauvegarde, l'abandon des processus en cours d'exécution et la libération des ressources verrouillées. Le mode maintenance est pris en charge dans les cellules individuelles, ainsi que dans les environnements MOM et cluster.

Démarrage du mode maintenance

Le mode maintenance peut être démarré par les utilisateurs ayant des droits d'administration via l'interface de ligne de commande. Pour démarrer le mode maintenance, exécutez :

Dans une cellule individuelle :

```
omnisv -maintenance [GracefulTime]
```

Dans un environnement MOM :

```
omnisv -maintenance -mom
```

D'après les instructions du Gestionnaire de cellule, les sessions en cours d'exécution doivent toutes s'arrêter en même temps, tandis que les cellules dans un environnement MOM entrent en mode maintenance individuellement.

Pour personnaliser la manière dont Gestionnaire de cellule entre en mode maintenance, modifiez les options globales appropriées. L'option `MaintenanceModeGracefulTime` reflète les secondes accordées aux services Data Protector pour abandonner les sessions en cours d'exécution, tandis que l'option `MaintenanceModeShutdownTime` reflète les secondes d'attente pour les sessions à abandonner. La valeur par défaut pour les deux options est de 300. Si l'option *`GracefulTime`* est utilisée, elle remplace l'option globale `MaintenanceModeGracefulTime`. Si une session de restauration est encore en cours d'exécution après le dépassement de cette option, le démarrage du mode maintenance échoue.

Si une cellule de l'environnement MOM échoue à entrer en maintenance, le mode est rétabli.

Pour vérifier si Data Protector est en cours d'exécution en mode maintenance, reportez-vous à l'état du service CRS en exécutant `omnisv -status`, ou vérifiez la barre d'état de l'interface utilisateur graphique. Notez que l'interface utilisateur graphique peut uniquement indiquer de manière fiable le mode maintenance lors de la connexion au Gestionnaire de cellule, ce qui peut parfois entraîner l'indication du mode maintenance sur la barre d'état même après que le Gestionnaire de cellule soit revenu au mode normal.

Au cours du mode maintenance, Gestionnaire de cellule refuse toutes les opérations d'écriture de données sur la base de données interne, comme la création de nouveaux périphériques, la sauvegarde et la restauration de sessions ou leurs tests, les sessions de purge, copie et consolidation.

Dans les environnements cluster, seules les activités liées au cluster manuel peuvent être effectuées lorsque le mode maintenance est actif, notamment l'arrêt des packages de cluster, l'arrêt des services Data Protector ou le montage de volume manuel.

Toutes les opérations IDB en lecture seule sont autorisées lorsque le mode maintenance est actif. Les services Data Protector sont tous opérationnels. Seuls les utilisateurs ayant des droits d'utilisateur administratif Data Protector peuvent se connecter à la cellule ou MOM lorsque le Gestionnaire de cellule est en mode maintenance.

Quitter le mode maintenance

Pour quitter le mode maintenance sur Gestionnaire de cellule à l'aide du CLI, exécutez :

- Dans une cellule individuelle :

  ```
  omnisv -maintenance -stop
  ```
- Dans un environnement MOM :

  ```
  omnisv -maintenance –mom_stop
  ```

Dans un environnement MOM, une cellule individuelle ne peut pas quitter le mode maintenance. La maintenance MOM peut uniquement être invoquée à partir du serveur MOM.

Pour quitter le mode maintenance à l'aide de l'interface utilisateur graphique :

1. Dans la liste de contexte, sélectionnez **Clients**.
2. Dans le menu **Actions**, cliquez sur **Arrêter le mode maintenance**.

Après la reprise du mode normal, vous pouvez redémarrer les sessions abandonnées et rejetées, car elle ont été consignées dans le fichier `maintenance.log`, localisé dans le répertoire par défaut des fichiers journaux Data Protector.

Les deux exemples suivants montrent les entrées `maintenance.log` pour les sessions abandonnées et rejetées :

```
10.5.2013 10:52:45  OMNISV.2492.9936
["/cli/omnisv/omnisv.c $Rev: 22709 $ $Date:: 2013-03-22 18:00:03":247] X.99.01 b2
Session was aborted - graceful period expired!
session id:        2013/05/10-8
session type:      0
datalist:          large_backup
start date:        2013-05-10 10:52:45
owned by:          JOHN.JOHNSON@company.com

10.5.2013 10:48:45  CRS.7620.3308 ["/cs/mcrs/sessions.c $Rev: 22709 $ $Date:: 2013-
03-22 18:00:03":142] X.99.01 b2
CRS is in maintenance mode - session rejected
session id:        R-2013/05/10-200
session type:      dbsm
session desc:      Database
start date:        2013-05-10 10:48:45
owned by:          .@ pid=0
```

Les sessions sont consignées comme abandonnées lorsqu'elles ont essayé de démarrer alors que le mode maintenance était actif. Pour exécuter les sessions abandonnées par la suite :

1. Dans la liste de contexte, cliquez sur **Base de données interne**
2. Dans la fenêtre de navigation, développez **Sessions**.
3. Faites un clic droit sur une session, puis sélectionnez **Redémarrer objets ayant échoué** dans le menu de contexte

Les sessions sont consignées comme rejetées lorsqu'elles ont essayé de démarrer alors que Gestionnaire de cellule entrait en mode maintenance. Pour exécuter les sessions rejetées ultérieurement, redémarrez manuellement chaque session.

Importation d'un client compatible cluster vers une cellule

Après avoir installé localement le logiciel Data Protector sur un client compatible cluster, importez le serveur virtuel représentant le client compatible cluster vers la cellule Data Protector.

Conditions préalables

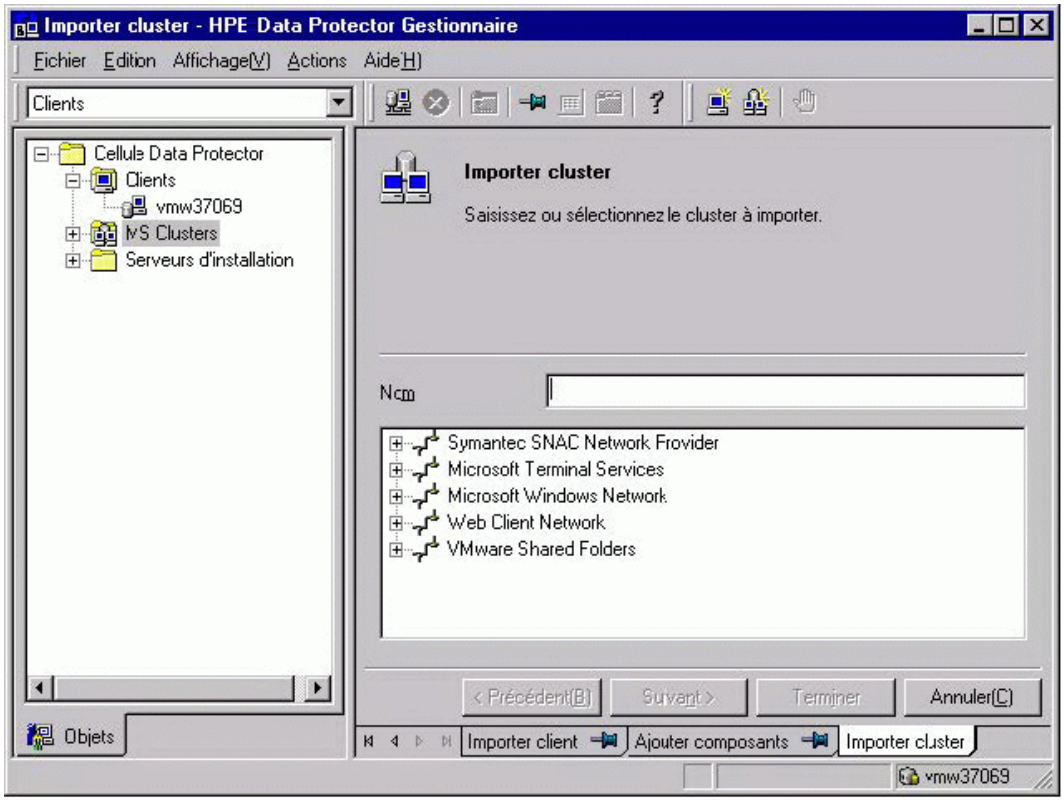
- Data Protector doit être installé sur tous les nœuds cluster.
- Tous les packages cluster doivent être exécutés dans le cluster.

Serveur de Cluster Microsoft

Pour importer un client de Microsoft Cluster Server vers la cellule Data Protector

1. Dans le Gestionnaire Data Protector, passez au 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. Tapez le nom du serveur virtuel représentant le client cluster à importer ou parcourez le réseau pour sélectionner le serveur virtuel.

   Importation d'un client Microsoft Cluster Server vers une cellule



4. Cliquez sur **Suivant**.
5. Cliquez sur **Terminer** pour importer le client cluster.

CONSEIL :
Pour importer un nœud de cluster spécifique ou un serveur virtuel, faites un clic droit dans la fenêtre de navigation et cliquez sur **Importer nœud cluster** ou **Importer serveur virtuel cluster**.

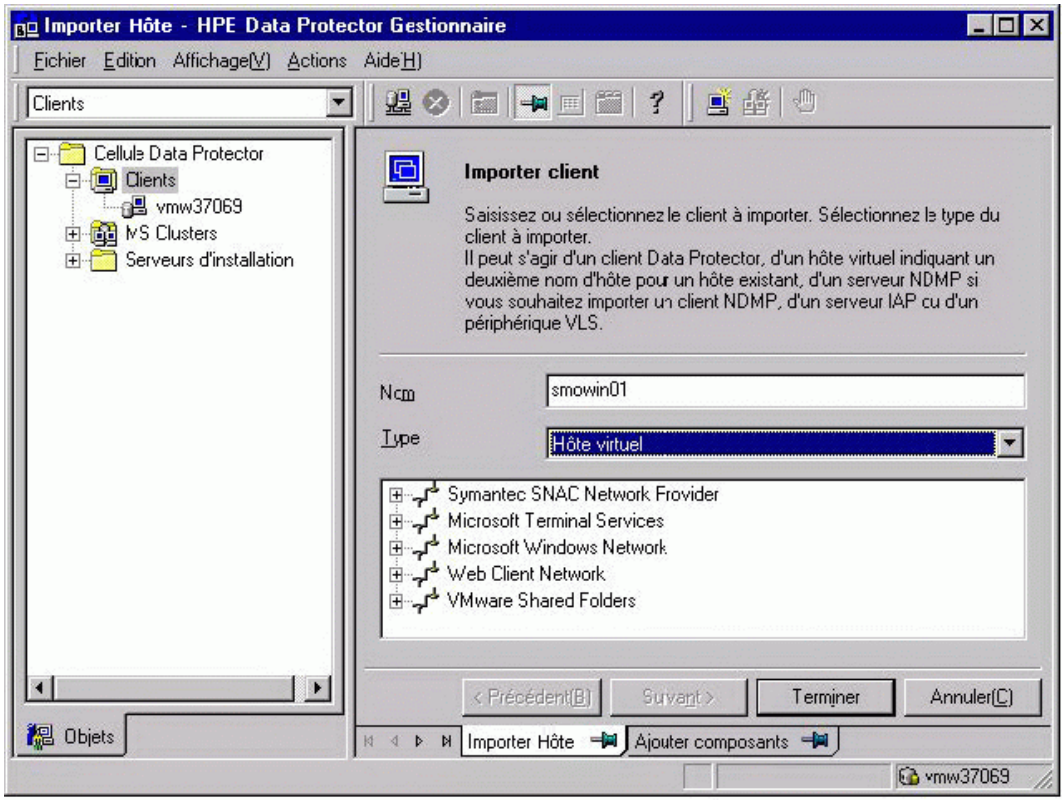
Autres clusters

Pour importer un clientServiceguard, Veritas ou IBM HACMP Cluster vers la cellule Data Protector

1. Dans le Gestionnaire Data Protector, passez au contexte Clients.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Clients** puis cliquez sur **Importer client**.
3. Tapez le nom d'hôte du serveur virtuel comme indiqué dans le package de cluster d'application, ou parcourez le réseau pour sélectionner le serveur virtuel (sur l'interface utilisateurs graphique Windows uniquement) que vous voulez importer.

   Sélectionnez l'option **Hôte virtuel** pour indiquer qu'il s'agit d'un serveur virtuel cluster.

   Importation d'un client Serviceguard ou Veritas vers une cellule



4. Cliquez sur **Terminer** pour importer le serveur virtuel.

CONSEIL :
Pour configurer les sauvegardes de données sur les disques locaux des nœuds cluster, vous devez importer les nœuds cluster représentant les clients Data Protector.

Exportation de clients d'une cellule

Exporter un client d'une cellule Data Protector signifie supprimer ses références de la base de données interne (IDB) du Gestionnaire de cellule sans désinstaller le logiciel du client. Ceci peut être réalisé à l'aide de l'interface utilisateur graphique Data Protector.

Vous pouvez vouloir utiliser la fonction d'exportation dans les cas suivants :

- Vous voulez déplacer un client vers une autre cellule
- Vous voulez supprimer un client de la configuration de cellule Data Protector qui ne fait plus partie du réseau
- Vous voulez résoudre les problèmes liés à l'attribution de licences

  Lorsque vous exportez un client d'une cellule, la licence devient disponible pour d'autres systèmes.

Conditions préalables

Avant d'exporter un client, vous devez vérifier ce qui suit :

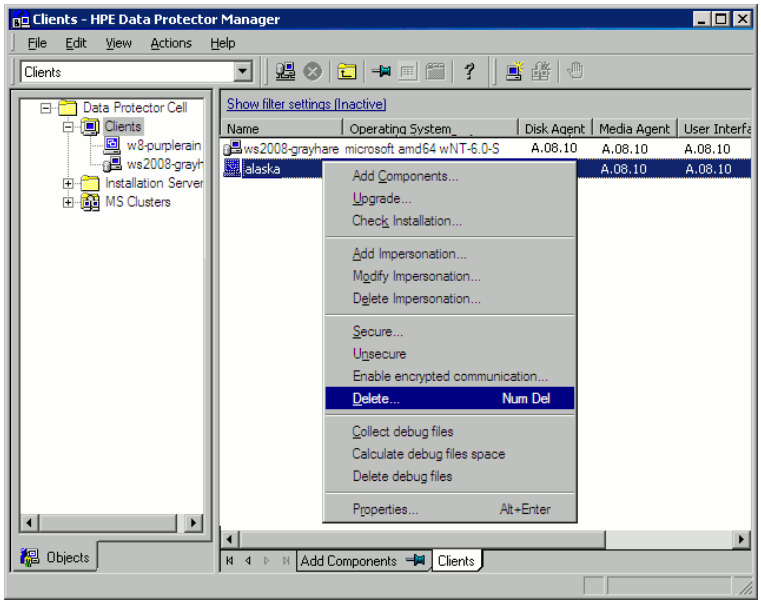
- Toutes les occurrences du client ont été supprimées des spécifications de sauvegarde. Dans le cas contraire, Data Protector essaiera de sauvegarder des clients inconnus et cette partie de la spécification de sauvegarde échouera. Pour plus d'informations sur la manière de modifier les spécifications de sauvegarde, consultez l'index *Aide de Data Protector* : "modification, spécification de sauvegarde".
- Le client ne dispose d'aucun périphérique de sauvegarde configuré et connecté ni de baies de disques. Lorsque le système est exporté, Data Protector ne peut plus utiliser ses périphériques de sauvegarde ou ses baies de disques dans la cellule originale.

Exportation d'un client

Pour exporter un client à l'aide de Data Protector GUI

1. Dans la liste de contexte, 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**.

Exportation d'un système client



3. Il vous sera demandé si vous souhaitez également désinstaller le logiciel Data Protector. Cliquez sur **Non** pour exporter le client, puis cliquez sur **Terminer**.

Le client est supprimé de la liste dans la zone de résultats.

> **REMARQUE :**
> Vous ne pouvez pas exporter ni supprimer de client Data Protector si le Gestionnaire de cellule est installé sur le même système que le client à exporter. Cependant, vous pouvez exporter les clients des systèmes où seuls le client et Serveur d'installation sont installés. Dans tous les cas, Serveur d'installation est également supprimé de la cellule.

Clients de Microsoft Cluster Server

Pour exporter un client Microsoft Cluster Server de la cellule Data Protector

1. Dans la liste de contexte, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, cliquez sur **MS Clusters**, cliquez avec le bouton droit de la souris sur le système client à exporter, puis cliquez sur **Supprimer**.
3. Il vous est demandé si vous voulez 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**.

À propos de la sécurité

Cette section décrit les éléments de sécurité de Data Protector. Elle décrit les paramètres avancés pouvant être utilisés pour améliorer la sécurité de Data Protector avec des conditions préalables et des éléments à prendre en considération :

Etant donné que l'amélioration de la sécurité à l'échelle d'un environnement tout entier implique la prise de mesures complémentaires, 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, l'ajout de clients et 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 œuvre dans des couches de sécurité critique différentes afin d'assurer le fonctionnement sécurisé de Data Protector. Ces couches sont les clients de Data Protector, Gestionnaire de cellule et les utilisateurs. Cette section explique comment configurer la sécurité sur chacune de ces couches.

Sécurité des clients

Les agents Data Protector installés sur les clients de la cellule offrent de puissantes fonctionnalités, notamment l'accès à toutes les données du système. Il est important que ces fonctionnalités sont uniquement disponibles sur les processus en cours d'exécution sur les **autorités de cellules** (Gestionnaire de cellule et Serveur d'installation), et que toutes les autres demandes sont rejetées.

Avant de sécuriser les clients, il est important de déterminer une liste des hôtes approuvés. Cette liste doit inclure :

- Gestionnaire de cellule
- Serveur d'installations appropriés
- Pour certains clients, également une liste de clients qui accèderont aux robots à distance.

> **IMPORTANT :**
> La liste doit contenir tous les noms d'hôte possibles (ou adresses IP) d'où les connexions peuvent provenir. Plusieurs noms d'hôte peuvent être nécessaires si l'un des clients ci-dessus est multirésident (possède plusieurs adaptateurs de réseau et/ou adresses IP) ou est un cluster.
>
> Si la configuration DNS dans la cellule n'est pas uniforme, des considérations supplémentaires peuvent s'appliquer.

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.

- Gestionnaire de cellule / Manager-of-Managers
- Serveur d'installations
- Clients Agent de support

> **REMARQUE :**
> Les clients de l'interface utilisateur n'ont pas besoin d'être ajoutés à la liste des clients fiables. En fonction des droits utilisateur, vous pouvez soit utiliser l'interface utilisateur graphique pour accéder à la fonctionnalité Data Protector complète soit accéder uniquement à des contextes spécifiques.

Utilisateurs Data Protector

Vous devez tenir compte de ces aspects importants lorsque vous configurez des utilisateurs Data Protector :

- Certains droits utilisateur sont très puissants. À titre d'exemple, les droits utilisateur `User configuration` et `Clients configuration` permettent à l'utilisateur de modifier les paramètres de sécurité. Le droit utilisateur `Restore to other clients` est également très puissant, notamment s'il est associé (mais pas uniquement) au droit `Back up as root` ou `Restore as root`.
- Même les droits utilisateur moins puissants comportent un risque inhérent associé. Data Protector peut être configuré pour limiter certains droits utilisateur afin de réduire ces risques. Ces paramètres sont décrits ultérieurement au cours de ce chapitre. Reportez-vous également à la rubrique Droit utilisateur Démarrer spécification de sauvegarde, Page 204.
- Data Protector est fourni avec seulement quelques groupes d'utilisateurs prédéfinis. Nous vous conseillons de définir des groupes spécifiques pour chaque type d'utilisateur dans l'environnement Data Protector afin de réduire au strict minimum les droits qui leur sont attribués.
- En plus d'attribuer les droits utilisateur par appartenance à un groupe d'utilisateurs, vous pouvez vouloir limiter davantage les actions de certains groupes d'utilisateurs à des systèmes spécifiques uniquement de la cellule Data Protector. Vous pouvez mettre en œuvre cette politique en configurant le fichier user_restrictions. Pour plus d'informations, voir *Aide de Data Protector*.
- La configuration des utilisateurs est liée à la validation utilisateur (voir Vérification stricte du nom d'hôte, Page suivante). Une validation optimisée peut être sans valeur sans une configuration utilisateur appropriée et vice-versa. Même la configuration utilisateur la plus soignée peut être contournée en l'absence d'une validation optimisée.
- Il est important que la liste d'utilisateurs Data Protector ne contienne pas d'utilisateurs "faibles".

  > **REMARQUE :**
  > La partie hôte d'une spécification d'utilisateur est la partie importante (particulièrement avec la validation améliorée), alors que les parties utilisateur et groupe ne peuvent pas être vérifiées de manière fiable. Tout utilisateur possédant des droits utilisateur puissants doit être configuré pour le client spécifique qu'ils utilisera pour l'administration de Data Protector. Si plusieurs clients sont utilisés, une entrée devra être ajoutée pour chaque client, plutôt que de spécifier un tel utilisateur en tant qu'utilisateur, groupe, <Tous>. Les utilisateurs non fiables ne doivent pas être autorisés à se connecter à l'un de ces systèmes.

Pour plus de détails sur la configuration des utilisateurs, voir l'index *Aide de Data Protector* : "configuration, utilisateurs".

Sécurité de Gestionnaire de cellule

Il est essentiel de garantir la sécurité de Gestionnaire de cellule car Gestionnaire de cellule a accès à l'ensemble des clients et des données de la cellule.

La sécurité de Gestionnaire de cellule peut être renforcée via la fonctionnalité de vérification stricte du nom d'hôte. Cependant, il est également important que le Gestionnaire de cellule soit sécurisé en tant que client et que la configuration des utilisateurs de Data Protector soit effectuée avec soin.

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.

Pour plus d'informations, voir Vérification stricte du nom d'hôte, bas.

Autres aspects de sécurité

Il existe également certains autres aspects de sécurité à prendre en compte :

- Les utilisateurs ne doivent pas avoir accès aux clients fiables (Gestionnaire de cellule, Serveur d'installations, MA et clients côté robotique). De plus, en accordant une connexion `anonymous` ou un accès en `ftp`, cela 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 à codage personnalisé. Notez qu'après la modification de l'encodage d'une bibliothèque, vous devez réaliser une sauvegarde complète.

Pour tout autre aspect lié à la sécurité, consultez le *Aide de Data Protector* et le *Guide conceptuel Data Protector*.

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 extrêmement facile à configurer et offre un niveau de sécurité raisonnable dans les environnements où la sécurité est considérée comme "consultative" (c'est-à-dire lorsque des malveillances sont peu probables).

D'autre part, le paramètre de vérification stricte du nom d'hôte offre une validation renforcée des utilisateurs. Le processus de validation utilise le nom d'hôte résolu par le Gestionnaire de cellule par la recherche DNS inverse à partir de l'adresse IP obtenue via la connexion. Cela impose les limitations et considérations suivantes :

Limites

- L'efficacité de la validation des utilisateurs en fonction de l'adresse IP est limitée à celle de la protection anti-usurpation instaurée dans le réseau. Le responsable de la sécurité doit déterminer si le réseau existant dispose d'un niveau de sécurité anti-usurpation suffisant pour des critères de sécurité spécifiques. La protection anti-usurpation peut être ajoutée par la segmentation du réseau à l'aide de pare-feu, 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 à haute sécurité, les utilisateurs normaux et les super utilisateurs ne doivent pas être mélangés dans le même client.
- Les hôtes utilisés dans des spécifications d'utilisateurs ne peuvent pas être configurés de manière à utiliser DHCP, sauf s'ils sont liés à une adresse IP fixe et configurés dans le système DNS.

N'oubliez pas ces limites afin d'évaluer correctement le degré de sécurité possible grâce à 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. Cette différence peut être délibérée ou indiquer une mauvaise configuration du client ou de la table DNS inverse.
- Le client est multirésident (possède plusieurs adaptateurs de réseau et/ou adresses IP). L'application ou non de cette remarque à un client multirésident particulier dépend de son rôle dans 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. Il faut vérifier les spécifications existantes des utilisateurs de Data Protector pour voir s'ils peuvent être concernés par l'une des explications ci-dessus. Selon le cas, il peut être nécessaire de modifier des spécifications existantes ou d'en ajouter des nouvelles au compte pour toutes les adresses IP d'où peuvent provenir les demandes de connexions.

Notez que les utilisateurs doivent être reconfigurés, même en cas de retour à la validation des utilisateurs par défaut, si vous avez dû modifier les spécifications d'utilisateurs lors de l'activation de la vérification stricte du nom d'hôte. Nous vous recommandons donc de décider de la méthode de validation des utilisateurs à employer et de continuer à l'utiliser.

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.

La configuration des utilisateurs avec des IP (à la place des noms d'hôte) pour la validation résout sans aucun doute certains problèmes potentiellement liés à la validation DSN, mais cette méthode est plus difficile à mettre en œuvre.

Conditions préalables

La validation renforcée ne garantit pas automatiquement l'accès à certaines connexions internes. C'est pourquoi, si cette validation est utilisée, un nouvel utilisateur doit être ajouté pour chacun des éléments suivants :

- Agent d'application (OB2BAR) sur les clients Windows. Pour les clients Windows, vous devez 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, reportez-vous à l'index *Aide de Data Protector* : "vérification stricte du nom d'hôte".

Pour plus d'informations sur la configuration des utilisateurs, voir l'index *Aide de Data Protector* : "configuration, utilisateurs".

Activation de la fonctionnalité

Pour activer la vérification stricte du nom d'hôte, définissez l'option globale `StrictSecurityFlags` sur `0x0001`.

Pour plus d'informations sur les options globales , reportez-vous au *Guide de dépannage Data Protector*.

Droit utilisateur Démarrer spécification de sauvegarde

Pour plus d'informations sur les utilisateurs Data Protector et les droits utilisateur, consultez l'index *Aide de Data Protector* : "utilisateurs".

Le droit utilisateur `Start backup specification` seul ne permet pas à un utilisateur d'exploiter le contexte de sauvegarde dans l'interface utilisateur graphique. L'utilisateur est autorisé à démarrer une spécification de sauvegarde à partir de la ligne de commande en utilisant l'omnib avec l'option -datalist.

> **REMARQUE :**
> En combinant les droits utilisateur `Start Backup Specification` et `Start Backup` , un utilisateur est autorisé à consulter les spécifications de sauvegarde configurées dans l'interface utilisateur graphique et peut démarrer une spécification de sauvegarde ou une sauvegarde interactive.

Autoriser les utilisateurs à effectuer des sauvegardes interactives n'est pas toujours souhaitable. Pour autoriser les sauvegardes interactives uniquement pour les utilisateurs qui ont également le droit d'enregistrer une spécification de sauvegarde, définissez l'option globale `StrictSecurityFlags` sur `0x0200`.

Pour plus d'informations sur les options globales, reportez-vous au *Guide de dépannage Data Protector.*

Masquage du contenu des spécifications de sauvegarde

Dans un environnement à haute sécurité, le contenu des spécifications de sauvegarde enregistrées peut être considéré comme des informations sensibles ou même confidentielles. Data Protector peut

être configuré pour masquer le contenu des spécifications de sauvegarde pour tous les utilisateurs, sauf ceux bénéficiant du droit utilisateur `Save backup specification`. Pour cela, définissez l'option globale `StrictSecurityFlags` sur `0x0400`.

Pour plus d'informations sur les options globales , reportez-vous au *Guide de dépannage Data Protector*.

Groupements d'hôtes approuvés

La fonctionnalité d'hôtes approuvés réduit le besoin d'accorder le droit utilisateur Restaurer vers autres clients aux utilisateurs quand ils ont uniquement besoin de restaurer les données d'un client vers un autre dans un nombre limité de clients. Vous pouvez définir des groupes d'hôtes qui se confieront les données.

Les groupements d'hôtes approuvés sont généralement utilisés dans les cas suivants :

- Pour les clients d'un cluster (nœuds et serveur virtuel).
- Si le nom d'hôte d'un client est modifié et si les données des anciens objets de sauvegarde doivent être restaurées.
- S'il existe un désaccord entre le nom d'hôte du client et les objets de sauvegarde à cause de problèmes avec le DNS.
- Si un utilisateur possède plusieurs clients et doit restaurer les données d'un client vers un autre.
- En cas de migration de données d'un hôte vers un autre.

Configuration

Pour configurer les groupement d'hôtes approuvés, sur l'instance Gestionnaire de cellule, créez le fichier *données_programme_Data_Protector*`\Config\Server\cell\host_trusts` (systèmes Windows) ou `/etc/opt/omni/server/cell/host_trusts` (systèmes UNIX).

Les groupes d'hôtes qui se confieront leurs données sont définis par des listes de noms d'hôtes 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 des difficultés à utiliser Data Protector, vous pouvez utiliser les informations contenues dans les fichiers journaux pour déterminer votre problème. Par exemple, les événements

consignés peuvent vous aider à déterminer les utilisateurs ou clients mal configurés.

Événements de sécurité des clients

Les événements de sécurité des clients sont consignés dans le fichier `inet.log` de chaque client de la cellule dans le répertoire par défaut des fichiers journaux Data Protector.

Événements de sécurité du Gestionnaire de cellule

Les événements de sécurité du Gestionnaire de cellule sont consignés dans le fichier `security.log` résidant dans le répertoire par défaut des fichiers journaux du serveur Data Protector.

Authentification utilisateur et LDAP

L'authentification et l'autorisation de Data Protector en tant que système d'entreprise doivent être connectées à l'infrastructure de gestion des utilisateurs de l'entreprise. Cette connexion permet aux utilisateurs et groupes configurés dans un annuaire d'utilisateurs de l'entreprise d'avoir accès aux services Data Protector.

L'authentification utilisateur se fait sur des connexions sécurisées, et Lightweight Directory Access Protocol (LDAP) sert de technologie sous-jacente. Par conséquence, les utilisateurs peuvent utiliser leurs justificatifs d'entreprise pour accéder à des services Data Protector et n'ont pas à maintenir des mots de passe séparés. De plus, les administrateurs ou opérateurs peuvent être maintenus dans des groupes dans l'annuaire de l'entreprise en adhérant à des processus d'autorisation et d'approbation établis.

L'intégration LDAP est configurée dans un domaine de sécurité du serveur d'application embarqué de Data Protector (WildFly) avec des modules de connexion Java Authentication and Authorization Service (JAAS). Un module de connexion LDAP optionnel propose des services d'authentification et d'autorisation LDAP, qui sont mappés sur les permissions Data Protectorpar un module de connexion Data Protector obligatoire. Si l'intégration LDA n'est pas configurée, alors Data Protector fonctionne comme dans les versions précédentes.

Data Protector utilise les modules de connexion en tant que pile de modules de connexion pour authentifier les utilisateurs. Lorsqu'un utilisateur se connecte au Gestionnaire de cellule avec l'interface utilisateur Data Protector, l'authentification utilisateur est effectuée par les modules de connexion suivants :

1. Module Connexion LDAP : Authentifie les justificatifs utilisateur, comme le nom d'utilisateur et le mot de passe, avec un serveur LDAP existant. Voir Initialisation et configuration du module de connexion LDAP.
2. Data ProtectorModule de connexion : Authentifie les justificatifs utilisateur en les comparant à la liste d'utilisateurs Data Protector et au mot de passe d'accès Web. Voir Accorder des permissions Data Protector aux utilisateurs ou groupes LDAP.
3. Après avoir effectué toutes les étapes nécessaires à la réalisation de l'initialisation et de la configuration de LDAP, vous pouvez aussi vérifier la configuration. Voir Vérifier la configuration LDAP.

> **REMARQUE :** Lorsqu'un utilisateur ou client est configuré dans Data Protector pour permettre l'accès CLI de façon classique, l'interface utilisateur graphique Data Protector n'utilise pas la fonctionnalité LDAP.

Initialisation et configuration du module de connexion LDAP

Le module de connexion LDAP se trouve dans le domaine de sécurité du serveur d'application WildFly, installé avec Data Protector. Le module de connexion LDAP doit être initialisé et configuré avant la première utilisation de la fonction de sécurité LDAP.

1. Initialisation du module de connexion LDAP.
2. Configuration du module de connexion LDAP.

Initialisation du module de connexion LDAP

Pour initialiser le module de connexion LDAP, utilisez l'utilitaire `jboss-cli`, qui est également installé avec Data Protector

1. Le dispositif `jboss-cli` se trouve dans : `%Data_Protector_home%/AppServer/bin`. Exécutez la commande suivante :
   - **Windows** : `jboss-cli.bat --file=ldapinit.cli`
   - **UNIX** : `jboss-cli.sh --file=ldapinit.cli`

   Cette commande crée un module de connexion LDAP en configuration WildFly et intègre des valeurs par défaut dans ce nouveau module de connexion. Les valeurs par défaut générées par la ligne de commande dans le fichier de configuration `standalone.xml`:

```
<security-domain name="hpdp-domain">
<authentication>
<login-module code="LdapExtended" flag="optional">
<module-option name="java.naming.factory.initial"
value="com.sun.jndi.ldap.LdapCtxFactory"/>
<module-option name="java.naming.security.authentication" value="simple"/>
<module-option name="roleFilter" value="(member={1})"/>
<module-option name="roleAttributeID" value="memberOf"/>
<module-option name="roleNameAttributeID" value="distinguishedName"/>
<module-option name="roleAttributeIsDN" value="true"/>
<module-option name="searchScope" value="SUBTREE_SCOPE"/>
<module-option name="allowEmptyPasswords" value="true"/>
<module-option name="password-stacking" value="useFirstPass"/>
</login-module>
<login-module code="com.hp.im.dp.cell.auth.DpLoginModule" flag="required">
<module-option name="password-stacking" value="useFirstPass"/>
```

```
</login-module>

</authentication>

</security-domain>
```

> **REMARQUE :**
> Les valeurs par défaut générées par la ligne de commande dans le fichier de configuration `standalone.xml` changent si Gestionnaire de cellule est installé sur l'environnement UNIX et utilise l'authentification LDAP. Voici les modifications :
>
> ```
> <login-module code="LdapExtended" flag="optional">
>
> <module-option name="java.naming.factory.initial"
> value="com.sun.jndi.ldap.LdapCtxFactory"/>
>
> <module-option name="java.naming.security.authentication" value="simple"/>
>
> <module-option name="roleFilter" value="(member={1})"/>
>
> <module-option name="roleAttributeID" value="memberOf"/>
>
> <module-option name="roleNameAttributeID" value="distinguishedName"/>
>
> <module-option name="roleAttributeIsDN" value="true"/>
>
> <module-option name="searchScope" value="SUBTREE_SCOPE"/>
>
> <module-option name="allowEmptyPasswords" value="false"/>
>
> <module-option name="password-stacking" value="useFirstPass"/>
>
> <module-option name="java.naming.provider.url" value="ldap://<IP_of_
> Active_Directory_host>"/>
>
> <module-option name="baseCtxDN" value="OU=_Benutzer,DC=godyo,DC=int"/>
>
> <module-option name="rolesCtxDN" value="OU=_Gruppen,DC=godyo,DC=int"/>
>
> <module-option name="bindDN" value="CN=backup-service,OU=_Service_
> Accounts,DC=godyo,DC=int"/>
>
> <module-option name="bindCredential" value="password"/>
>
> <module-option name="baseFilter" value="(userPrincipalName={0})"/>
>
> </login-module>
> ```
>
> Les paramètres de configuration `baseCtxDN` et `rolesCtxDN` sont les principaux. Le paramètre d'unité d'organisation (UO) est utilisé pour authentifier le Gestionnaire de celluleUNIX.

2. Pour accéder à la console d'administration WildFly, située dans le Gestionnaire de cellule, à partir d'un client distant, activez l'accès à distance à la console d'administration WildFly. Pour cela, utilisez un éditeur de texte et modifier l'adresse de l'interface de gestion de 127.0.0.1 à 0.0.0.0 dans la section interface du fichier `standalone.xml` :

   ```
   <interfaces>

   <interface name="management">
   ```

```
<inet-address value="${jboss.bind.address.management:0.0.0.0}"/>
</interface>
<interface name="public">
<inet-address value="0.0.0.0"/>
</interface>
<interface name="unsecure">
<inet-address value="${jboss.bind.address.unsecure:127.0.0.1}"/>
</interface>
</interfaces>
```

3. Redémarrez les services Data Protector :

```
arrêtez omnisv
 et démarrez omnisv
```

Configuration du module de connexion LDAP

Afin de configurer le module de connexion LDAP, utilisez la console Admin Web du serveur d'application WildFly, qui est installée conjointement à Data Protector. Procédez comme suit :

1. Pour accéder à a console d'administration WildFly, créez un utilisateur WildFly. Pour créer un utilisateur WildFly, exécutez l'utilitaire d'ajout d'utilisateur :
   - **Windows** : `add-user.bat` situé dans `%Data_Protector_home%/AppServer/bin`
   - **UNIX** : `add-user.sh` situé dans `/opt/omni/AppServer/bin`
2. Fournit des résultats pour les paramètres suivants :
   - **Type d'utilisateur à ajouter** : Sélectionnez l'utilisateur de gestion.
   - **Domaine** : Laissez ce champ vide, car la valeur par défaut ManagementRealm est sélectionnée par l'utilitaire.
   - **Nom d'utilisateur** : Ajoutez un nom d'utilisateur.
   - **Mot de passe** : Ajoutez un mot de passe.
   - **Groupe** : Aucun
3. Pour accéder à la console d'administration WildFly, utilisez un navigateur et ouvrez l'URL : <http://cell-manager-name:9990/console>
4. Sur l'écran Authentification, indiquez le **Nom d'utilisateur** et **Mot de passe** créé à l'aide de l'utilisateur d'ajout d'utilisateur.
5. Cliquez sur **Se connecter**. La console Admin du serveur d'application WildFly apparaît.
6. Dans la console Admin WildFly, sélectionnez l'onglet **Profil**.
7. Dans l'onglet **Profil**, développez le nœud **Sécurité** puis cliquez sur **Domaines de sécurité**.

8. Dans la liste des domaines de sécurité enregistrés, cliquez sur **Affichage** pour hpdp-domain. Les modules de connexion suivants sont définis pour le domaine de sécurité, hpdp-domain :
   - LdapExtended
   - Com.hp.im.dp.cell.auth.DpLoginModule
9. Sélectionnez le module **LdapExtended**.
10. Dans la section Détails, cliquez sur l'onglet **Options du module**. Toutes les options du module préconfigurées sont répertoriées dans l'onglet **Options du module**.
11. Afin de personnaliser et d'utiliser le module de connexion LDAP, vous devez ajouter des options de module supplémentaires. Cliquez sur **Ajouter** et indiquez le **Nom** et la **Valeur** de chaque option du module. Pour plus d'informations, consultez le tableau suivant :

Option du module	Nom	Valeur	Description
URL du fournisseur	`java.naming.provider.url`	Spécifiez l'URL du serveur LDAP au format suivant : `ldap://<server>:<port>`	Un nom de propriété standard
Nom distinctif (DN) selon le contexte	`baseCtxDN`	Indiquez le DN de l'emplacement LDAP qui contient les utilisateurs.	Le DN fixe du contexte à partir duquel vous démarrez la recherche d'utilisateur
Filtre de base	`baseFilter`	Spécifiez l'attribut dans la configuration LDAP qui correspond au nom de connexion de l'utilisateur au format suivant : `(<user-login-name-attribute>={0})` où le `<user-login-name-attribute>` doit être remplacé par le nom de l'attribut LDAP correspondant.	Un filtre de recherche permettant de localiser le contexte de l'utilisateur à authentifier
DN de contexte des rôles	`rolesCtxDN`	Indiquez le DN de l'emplacement LDAP qui contient les groupes d'utilisateurs.	Le DN fixe du contexte à rechercher pour les groupes d'utilisateurs
DN associé	`bindDN`	Spécifiez le DN d'un utilisateur LDAP utilisé par le module de connexion pour	Le DN utilisé pour la liaison au serveur LDAP pour les requêtes

Option du module	Nom	Valeur	Description
		exécuter la liaison LDAP initiale. Vous devez disposer des autorisations requises pour rechercher l'emplacement LDAP des utilisateurs et des groupes afin d'obtenir les utilisateurs et leurs groupes. Ces emplacements sont définis dans le `baseCtxDN` et les options du module `rolesCtxDN` .	d'utilisateur et de rôles. Il s'agit d'un DN avec des droits lecture/recherche sur les valeurs `baseCtxDN` et `rolesCtxDN`
Informations d'identification de liaison	`bindCredential`	Spécifiez le mot de passe de l'utilisateur LDAP fourni dans l'option de module `BindDN`.	Mot de passe pour le `bindDN`

Pour plus d'informations sur les autres Options du module, consultez les URL suivantes :

- https://community.jboss.org/wiki/LdapExtLoginModule
- http://technet.microsoft.com/en-us/library/cc773354 (v=ws.10).aspx

12. Les modifications prendront effet une fois la configuration WildFly Application Server rechargée. Pour recharger la configuration, utilisez l'utilitaire `jboss-cli` situé dans : `%Data_Protector_home%/AppServer/bin`
13. Exécutez la commande suivante :
    - **Windows** : `jboss-cli.bat -c :reload`
    - **UNIX** : `jboss-cli.sh -c :reload`

> **REMARQUE :** Lors de la configuration du module de connexion LDAP dans les environnements MoM, n'oubliez pas d'exécuter les étapes ci-dessus sur chaque Gestionnaire de cellule. Chaque Gestionnaire de cellule dans l'environnement MoM doit avoir la même configuration pour le module de connexion LDAP.

Accorder des permissions Data Protector aux utilisateurs ou groupes LDAP

Les utilisateurs ne peuvent se connecter à un Gestionnaire de cellule que s'ils obtiennent les permissions Data Protector. Après avoir configuré le module de connexion LDAP, vous pouvez accorder les permissions Data Protector requises aux utilisateurs LDAP.

Pour accorder les permissions Data Protector, procédez comme suit :

1. Démarrez l'interface utilisateur Data Protector et accordez les permissions Data Protector aux utilisateurs ou groupes LDAP.

- Ajouter des utilisateurs LDAP aux groupes d'utilisateurs Data Protector.
- Ajouter des groupes LDAP aux groupes d'utilisateurs Data Protector.

2. Se connecter avec les informations d'identification LDAP.

Ajouter des utilisateurs LDAP à des groupes d'utilisateurs

Pour ajouter des utilisateurs LDAP à des groupes d'utilisateurs Data Protector, procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Utilisateurs.**
2. Dans la fenêtre de navigation, développez **Utilisateurs** et faites un clic droit sur le groupe d'utilisateurs auquel vous souhaitez ajouter les utilisateurs LDAP.
3. Cliquez sur **Ajouter/Supprimer utilisateurs** pour lancer l'assistant.
4. Dans l'onglet **Manuel** de la boîte de dialogue Ajouter/Supprimer utilisateurs, fournissez les détails suivants :
   - **Type** : Sélectionner LDAP.
   - **Nom** : Indiquez l'utilisateur LDAP au format de nom principal des utilisateurs LDAP.
   - **Entité** : Saisissez l'utilisateur LDAP.
   - **Description** : Cela est optionnel.
5. Cliquez sur **Terminer** pour quitter l'assistant.

Ajouter des groupes LDAP à des groupes d'utilisateurs

Pour ajouter des groupes LDAP à des groupes d'utilisateurs Data Protector, procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Utilisateurs.**
2. Dans la fenêtre de navigation, développez **Utilisateurs** et faites un clic droit sur le groupe d'utilisateurs auquel vous souhaitez ajouter les groupes LDAP.
3. Cliquez sur **Ajouter/Supprimer utilisateurs** pour lancer l'assistant.
4. Dans l'onglet **Manuel** de la boîte de dialogue Ajouter/Supprimer utilisateurs, fournissez les détails suivants :
   - **Type** : Sélectionner LDAP.
   - **Nom** : Indiquez le nom de groupe LDAP au format de nom distinctif (DN).
   - **Entité** : Saisissez le groupe LDAP.
   - **Description** : Cela est optionnel.
5. Cliquez sur **Terminer** pour quitter l'assistant.

> **REMARQUE :** Un utilisateur LDAP se voit automatiquement accorder le même niveau de permission que le groupe LDAP auquel il appartient.

Se connecter avec des justificatifs LDAP

Pour vous connecter avec vos justificatifs LDAP, procédez comme suit :

1. Démarrez l'interface utilisateur graphique Data Protector et connectez-vous à un Gestionnaire de cellule.
2. Sur l'écran d'authentification LDAP, fournissez les justificatifs LDAP pour accéder à Data Protector. L'utilisateur LDAP peut appartenir à tout groupe d'utilisateurs Data Protector disponible.

Vérifier la configuration LDAP

La procédure suivante explique comment vérifier si les droits utilisateur sont correctement définis pour un utilisateur ou groupe LDAP spécifique en interrogeant le fournisseur de service de connexion de Data Protector `getDpAcl`à partir d'un navigateur Web.

Pour obtenir la liste de contrôle d'accès (ACL) de Data Protector pour un utilisateur spécifique, procédez comme suit :

1. Connectez-vous au service Web du fournisseur de connexion Data Protector à l'aide d'un navigateur.
2. Il est possible que le navigateur vous invite à accepter le certificat de serveur. Cliquez sur **Accepter** pour confirmer la demande.
3. Une boîte de dialogue s'affiche, vous invitant à saisir les informations d'identification. Saisissez un nom d'utilisateur et mot de passe LDAP valides, qui ont été configurés à l'aide de Data Protector. Voir Configuration du mode de connexion LDAP.
4. Le navigateur affiche la liste de contrôle d'accès (ACL) suivante : `https://<server>:7116/dp-loginprovider/restws/dp-acl`
5. Utilisez la ACL pour vérifier si les droits attribués correspondent aux droits utilisateur Data Protector spécifiés pour le groupe d'utilisateurs Data Protector correspondant.

Utilitaire de création de certificats

L'utilitaire de création de certificats X.509 `omnigencert.pl` génère le serveur d'autorité des certificats (CA), et les certificats client et serveur. Il est responsable de la réalisation des tâches suivantes :

- Configuration d'un CA racine à niveau unique
- Création du CA et des certificats serveur et client
- Création de la structure de répertoires nécessaire pour le stockage des fichiers des clés, certificats, configurations et banques de clés.
- Stockage des certificats générés dans des emplacements prédéfinis sur le CM
- Création des fichiers de propriétés des rôles de service Web

> **REMARQUE :** L'utilitaire `omnigencert.pl` peut être exécuté uniquement par l'administrateur (Windows) ou l'utilisateur root (UNIX).

L'utilitaire `omnigencert.pl` est développé en tant que script et est installé avec le kit d'installation du gestionnaire de cellule (CM). Dans le cadre de l'installation du CM, le script est exécuté pour la première fois, et les certificats sont générés et stockés dans des emplacements prédéfinis.

Le script `omnigencert.pl` existe à l'emplacement suivant :

Windows : `%Data_Protector_home%\bin`

Unix :`/opt/omni/sbin`

Si nécessaire, les administrateurs Data Protector peuvent exécuter cet utilitaire à tout moment après l'installation pour recréer des certificats avec la nouvelle paire de clés de la nouvelle configuration de CA. Cependant, il n'est pas obligatoire d'utiliser les certificats générés par cet utilitaire pour l'authentification basée sur serveur. Au lieu de cela, vous pouvez utiliser une configuration de CA existante pour créer les certificats nécessaires.

Syntaxe

Cet utilitaire est initialement exécuté par le programme d'installation dans le cadre de l'installation du Gestionnaire de cellule et les certificats nécessaires sont créés et stockés à des emplacements prédéfinis.

L'utilisation de cet utilitaire est restreinte aux administrateurs et sert également à recréer des certificats avec une nouvelle paire de clés comprenant même la nouvelle configuration de CA. L'utilisateur « Administrator » de la plateforme Windows et « root » dans la plateforme UNIX peuvent exécuter ce script.

Le script `omnigencert.pl` existe à l'emplacement suivant :

Windows : `%Data_Protector_home%\bin`

Unix : `/opt/omni/sbin`

Vous pouvez exécuter l'utilitaire `omnigencert.pl` en utilisant la syntaxe et les options qui suivent :

Utilisation

```
[-no_ca_setup]

[-server_id ServerIdentityName]

[-user_ID UserIdentityName]

[-store_password KeystorePassword]

[-cert_expire CertificateExpireInDays]

[-ca_dn CertificateAuthorityDistinguishedName]

[-server_dn ServerDistinguishedName]

[-client_dn ClientDistinguishedName]

[-server_san]
```

L'utilitaire `omnigencert.pl` prend en charge plusieurs options, qui proposent de la flexibilité lors de la création de certificats. Si aucune option n'est indiquée, l'utilitaire utilise les valeurs par défaut pour créer les certificats.

L'utilitaire `omnigencert.pl` prend en charge les options suivantes :

Option	Description
-no_ca_setup	Crée les certificats client et serveur pour une configuration de CA existante. Cette option est invalide si aucune configuration de CA n'existe.
-server_id	Indique la valeur de l'entité de nom commun (CN) dans la section Nom distinctif (DN) du certificat serveur. La valeur par défaut pour cette option est le nom de domaine complet (FQDN) du CM.
-user_id	Indique la valeur de l'entité CN dans la section DN du certificat client. La valeur par défaut pour cette option est l'utilisateur du service Web.
-store_password	Définit le mot de passe pour la banque de clés ou banque d'approbations où se trouvent les certificats client et serveur, dont leurs clés. Si cette option n'est pas proposée, le mot de passe par défaut est utilisé pour créer les banques.
-cert_expire	Définit l'expiration du certificat généré en jours. La valeur par défaut pour cette option est 8 760 jours (24 ans).
-ca_dn	Définit la chaîne DN pour le CA. Le format de DN est le suivant : "CN=<valeur>, O=<valeur>, ST=<valeur>, C=<valeur>" CN = Nom commun, O=Nom organisation, ST=Nom État, C=Nom pays. Les valeurs par défaut pour les paramètres O, ST et C sont les suivantes : CN = CA <nom FDQN du serveur CM> O = HEWLETT-PACKARD ST = CA C= US
-server_dn	Définit la chaîne DN pour le certificat serveur. Le format de DN est le suivant : "CN=<valeur>, O=<valeur>, ST=<valeur>, C=<valeur>" CN = Nom commun, O=Nom organisation, ST=Nom État, C=Nom pays. Les valeurs par défaut pour les paramètres O, ST et C sont les suivantes : CN = <nom FDQN du serveur CM> O = HEWLETT-PACKARD ST = CA C= US
-client_dn	Définit la chaîne DN pour le certificat client ou utilisateur. Le format de DN est le suivant : "CN=<valeur>, O=<valeur>, ST=<valeur>, C=<valeur>" CN = Nom commun, O=Nom organisation, ST=Nom État, C=Nom pays. Les valeurs par défaut pour les paramètres O, ST et C sont les suivantes : CN = Utilisateur service Web O = HEWLETT-PACKARD ST = CA C= US

Option	Description

`-server_san`	Indique les noms alternatifs du sujet (SAN) dans le certificat serveur. Cependant, le certificat serveur généré lors de l'installation d'un Gestionnaire de cellule dispose d'entrées de type DNS dans la section SAN. Ces entrées SAN sont générées automatiquement sur la base des numéros IP disponibles dans le Gestionnaire de cellule. Pour écraser la création automatique d'entrées SAN dans le certificat serveur, indiquez cette option lors de la création de certificats avec l'utilitaire de création de certificats.
	Les types DNS et IP d'entrées SAN sont pris en charge.
	Le format de la valeur de cette option est le suivant :`santype:value,santype:value`
	Chaque entrée SAN est séparée par une virgule (",") et contient 2 parties : 1) Type de SAN et 2) valeur du type de SAN.
	Exemples :
	`dns:myserver1.mycompany.com, dns:myserver2.mycompany.com`
	`ip:10.218.1.100, ip:10.218.1.200, ip:10.218.1.155`
	`dns:myserver1.mycompany.com, ip:10.218.1.100`

REMARQUE :
L'utilitaire ne prend pas en charge les combinaisons suivantes pour les options :

- `-server_id` et `-server_dn`
- `-user_id` et `-client_dn`
- `-no_ca_setup` et `-ca_dn`.

Exemples

Les sections suivantes répertorient des commandes d'exemple pour exécuter l'utilitaire `omnigencert.pl` sur Windows et UNIX.

Le script `omnigencert.pl` existe à l'emplacement suivant :

Windows : `%Data_Protector_home%\bin`

Unix : `/opt/omni/sbin`

Commandes Windows et Unix

Tâche	Commande Windows	Commande Unix
Pour configurer le CA et générer les certificats CA, client et serveur avec les valeurs par défaut	%Data_Protector_home%\bin\perl.exe omnigencert.pl	/opt/omni/bin/perl omnigencert.pl
Pour configurer le CA et générer les certificats CA, client et serveur avec des valeurs de noms communs	%Data_Protector_home%\bin\perl.exe omnigencert.pl -server_id <value> -user_id <value>	/opt/omni/bin/perl omnigencert.pl -server_id <value> -user_id <value>
Pour configurer le CA et générer les certificats CA, client et serveur avec un mot de passe de banque spécifié	%Data_Protector_home%\bin\perl.exe omnigencert.pl -store_password <value>	/opt/omni/bin/perl omnigencert.pl -store_password <value>
Pour configurer le CA et générer les certificats CA, client et serveur avec le nombre de jours avant expiration spécifié	%Data_Protector_home%\bin\perl.exe omnigencert.pl -cert_expire <value>	/opt/omni/bin/perl omnigencert.pl -cert_expire <value>
Pour générer les certificats client et serveur avec une configuration CA existante (créée lors de l'installation) avec les valeurs par défaut	%Data_Protector_home%\bin\perl.exe omnigencert.pl –no_ca_setup	/opt/omni/bin/perl omnigencert.pl –no_ca_setup
Pour configurer le CA et générer les certificats CA, client et serveur avec les DN spécifiés	%Data_Protector_home%\bin\perl.exe omnigencert.pl -ca_dn <value> -server_dn <value>	/opt/omni/bin/perl omnigencert.pl -ca_dn <value> -server_dn <value> -client_dn

Tâche	Commande Windows	Commande Unix
	-client_dn <value>	<value>
Pour créer les certificats client et serveur avec une configuration de CA existante à l'aide des DN spécifiés.	%Data_Protector_home%\ bin\perl.exe omnigencert.pl -no_ca_setup -server_dn <value> -client_dn <value>	/opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_dn <value> -client_dn <value>
Pour créer les certificats client et serveur avec un certificat CA existant dans l'environnement SG-CLUSTER	1. Extrayez le mot de masse du magasin de clés existant à partir de <DP_DATA_ DIR>\Config\client\components \webservice.properties. 2. Extrayez la valeur **PGOSUSER** à partir de <DP_SDATA_ DIR>\server\idb\idb.config. 3. Exécutez l'utilitaire omnigencert.pl avec le nom du système virtuel de clusters comme suit : %Data_Protector_ home%\bin\perl.exe omnigencert.pl –no_ca_setup -server_id cm_virtual_ name.domain.com -user_id hpdp_so_user -store_password existing_keystor_passwd	1. Extrayez le mot de masse du magasin de clés existant à partir de /etc/opt/omni/client/components /webservice.properties. 2. Extrayez la valeur **PGOSUSER** à partir de /etc/opt/omni/server/ idb/idb.config.. 3. Exécutez l'utilitaire omnigencert.pl avec le nom du système virtuel de clusters comme suit : /opt/omni/bin/perl omnigencert.pl –no_ca_setup -server_id cm_virtual_ name.domain.com -user_id hpdp_so_user -store_password existing_ keystor_passwd
Pour créer les certificats CA, client et serveur dans l'environnement SG-CLUSTER	1. Extrayez le mot de masse du magasin de clés existant à partir de <DP_DATA_ DIR>\Config\client\components\ webservice.properties. 2. Extrayez la valeur **PGOSUSER** à partir de <DP_SDATA_ DIR>\server\idb\idb.config. 3. Exécutez l'utilitaire	1. Extrayez le mot de masse du magasin de clés existant à partir de /etc/opt/omni/client/ components/webservice.properties . 2. Extrayez la valeur **PGOSUSER** à partir de /etc/opt/omni/server/ idb/idb.config.

Tâche	Commande Windows	Commande Unix
	omnigencert.pl avec le nom du système virtuel de clusters comme suit : %Data_Protector_home%\bin\perl.exe omnigencert.pl -server_id cm_virtual_name.domain.com -user_id hpdp_so_user -store_password existing_keystor_passwd	3. Exécutez l'utilitaire omnigencert.pl avec le nom du système virtuel de clusters comme suit : /opt/omni/bin/perl omnigencert.pl -server_id cm_virtual_name.domain.com -user_id hpdp_so_user -store_password existing_keystor_passwd
Pour générer un certificat serveur avec des entrées SAN de type DNS pour un serveur de Gestionnaire de cellule spécifique.	%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn myserver3.mycompany.com -server_san "dns:myserver3.mycompany.com,dns:myserver3.mycompany.com"	/opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_dn myserver3.mycompany.com -server_san "dns:myserver3.mycompany.com, dns:myserver3.mycompany.com"
Pour générer un certificat serveur avec des entrées SAN de type IP pour un serveur de Gestionnaire de cellule spécifique.	%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn 10.218.1.100 -server_san “ip:10.218.1.100, ip:10.218.1.101, ip:10.218.1.125, ip:10.218.1.116”	/opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_dn 10.218.1.100 -server_san "ip:10.218.1.100, ip:10.218.1.101, ip:10.218.1.125, ip:10.218.1.116"
Pour générer un certificat serveur avec des entrées SAN de type IP et DNS pour un serveur de Gestionnaire de cellule spécifique.	%Data_Protector_home%\bin\perl.exe omnigencert.pl -no_ca_setup -server_dn myserver4.mycompany.com -server_san "dns:myserver4.mycompany.com, myserver4.mycompany.com,	/opt/omni/bin/perl omnigencert.pl -no_ca_setup -server_dn myserver4.mycompany.com -server_san "dns:myserver4.mycompany.com, myserver3.mycompany.com,

Tâche	Commande Windows	Commande Unix
	ip:10.218.1.100, ip:10.218.1.101, ip:10.218.1.125, ip:10.218.1.116"	ip:10.218.1.100, ip:10.218.1.101, ip:10.218.1.125, ip:10.218.1.116"

Structure de répertoires

Les sections suivantes répertorient les répertoires dans lesquels les certificats sont stockés.

Répertoire Windows	Répertoire Unix	Description
ProgramData\Omniback\Config\Server\certificates	/etc/opt/omni/server/certificates	Contient le fichier de certificat CA, cacert.pem, qui contient la clé publique CA.
ProgramData\Omniback\Config\Server\certificates\ca	/etc/opt/omni/server/certificates /ca	Contient la configuration, l'entrée et les autres fichiers nécessaires au fonctionnement du CA.
ProgramData\Omniback\Config\Server\certificates\ca\keys	/etc/opt/omni/server/certificates /ca/keys	Contient le fichier de clés privées de CA, cakey.pem.
ProgramData\Omniback\Config\Server\certificates\server	/etc/opt/omni/server/certificates /server	Contient deux types de banques : banques de clés et banques d'approbations. Ces banques sont créées par l'utilitaire Java, keytool, pour la protection des certificats du serveur et de ses clés. Ces banques sont protégées par le mot de passe de la banque. Il contient les banques suivantes : ca.truststore server.keystore server.truststore
ProgramData\Omniback\Config\Server\certificates\client	/etc/opt/omni/server/certificates /client	Contient deux types de banques : banques de clés et banques d'approbations.

Répertoire Windows	Répertoire Unix	Description
		Ces banques sont créées par l'utilitaire Java, keytool, pour la protection des certificats du client et de ses clés. Ces banques sont protégées par le mot de passe de la banque. Il contient les banques suivantes : • `client.keystore` • `client.truststore`
`ProgramData\Omniback\Config\Server\AppServer`	`/etc/opt/omni/server/AppServer`	Contient les fichiers de propriétés créés par cette utilitaire. Ce répertoire contient d'autres fichiers en plus des fichiers de propriétés suivants : • `jce-webservice-roles.properties` • `dp-webservice-roles.properties`

Écraser des certificats existants

Pour remplacer les certificats existants (générés par l'utilitaire dans le cadre de l'installation CM) par les certificats générés par une configuration CA existante, vous pouvez utiliser l'une des options suivantes :

- Écraser des certificats dans des fichiers de banques de clés et de banques d'approbations existants
- Écraser des certificats en créant des fichiers de banques de clés et de banques d'approbations

> **REMARQUE :** Après la recréation de certificats ou l'utilisation de nouveaux certificats, vous devez redémarrer les services Data Protector sur CM. Vous devez faire cela avant d'exécuter toute opération utilisant des certificats, car le redémarrage des services garantit que les nouveaux certificats sont appliqués.

Écraser des certificats dans des fichiers de banques de clés et de banques d'approbations existants

Pour écraser des certificats dans des fichiers de banques de clés et de banques d'approbations existants, effectuez les tâches suivantes :

- Remplacer les fichiers de banque client et serveur existants
- Remplacer le certificat CA
- Mettre à jour la chaîne de nom distinctif (DN)

Remplacer les fichiers de banque client et serveur existants

Pour remplacer les fichiers de banque client et serveur existants, procédez comme suit :

1. Retrouvez le mot de passe des banques de clés et d'approbations depuis les fichiers de configuration `webservice.properties` et `standalone.xml` , situés dans :

   Windows

   - `ProgramData\OmniBack\Config\client\components\webservice.properties`
   - `ProgramData\OmniBack\Config\server\AppServer\standalone.xml`

   UNIX

   - `/etc/opt/omni/client/components/webservice.properties`
   - `/etc/opt/omni/server/AppServer/standalone.xml`

2. Supprimez toutes les entrées des fichiers de banque client et serveur existants `server.keystore`, `server.truststore`, `client.keystore` et `client.truststore`, situés dans :

   Serveur

   - Windows : `ProgramData\Omniback\Config\Server\certificates\server`
   - Unix : `/etc/opt/omni/server/certificates/server`

   Client

   - Windows : `ProgramData\Omniback\Config\Server\certificates\client`
   - UNIX : `/etc/opt/omni/server/certificates/client`

   Pour effectuer ces modifications, vous pouvez utiliser l'utilitaire Java keytool, situé dans :

   Windows : `Program Files\Omniback\jre\bin`

   UNIX : `/opt/omni/jre/bin`

3. Importez les certificats générés dans les banques suivantes avec l'utilitaire Java keytool :
   - Certificats serveur et CA dans `server.keystore`
   - Certificat CA et client dans `server.truststore`
   - Certificat CA dans `ca.truststore`
   - Certificats client et CA dans `client.keystore`
   - Certificat CA et serveur dans `client.truststore`

Remplacer le certificat CA

Pour remplacer le certificat CA existant, procédez comme suit :

1. Notez les permissions du fichier de certificat CA existant `cacert.pem`, situé dans :
   - **Windows** : `ProgramData\Omniback\Config\Server\certificates`
   - **UNIX** : `/etc/opt/omni/server/certificates`
2. Remplacez le fichier de certificat CA existant `cacert.pem` par le certificat CA généré.

Mettre à jour la chaîne de nom distinctif (DN)

Remplacez la chaîne de nom distinctif (DN) dans les fichiers `jce-webservice-roles.properties` et `dp-webservice-roles.properties` par la chaîne DN utilisée pour le certificat client. Ces fichiers se trouvent dans :

Windows : `ProgramData\Omniback\Config\Server\AppServer`

UNIX : `/etc/opt/omni/server/AppServer`

> **REMARQUE :** Dans la chaîne DN, ajoutez un backslash (\) avant les espaces et le caractère « = ».

Écraser des certificats en créant des fichiers de banques de clés et de banques d'approbations

Pour écraser des certificats dans des nouveaux fichiers de banques de clés et de banques d'approbations, effectuez les tâches suivantes :

- Remplacer les fichiers de banque client et serveur existants
- Remplacer le certificat CA
- Mettre à jour la chaîne de nom distinctif (DN)
- Mettre à jour le fichier de configuration avec le mot de passe de la banque

> **REMARQUE :** Vous devez conserver le mot de passe pour les banques client et serveur.

Remplacer les fichiers de banque client et serveur existants

Pour remplacer les fichiers de banque client et serveur existants, procédez comme suit :

1. Notez les permissions des fichiers de banque client et serveur existants `server.keystore`, `server.truststore`, `client.keystore` et `client.truststore`, situés dans :

   Serveur

   - Windows : `ProgramData\Omniback\Config\Server\certificates\server`
   - UNIX : `/etc/opt/omni/server/certificates/server`

Client

- Windows : `ProgramData\Omniback\Config\Server\certificates\client`
- UNIX : `/etc/opt/omni/server/certificates/client`

2. Supprimez les fichiers de banque client et serveur.
3. Créez des boutiques avec les mêmes noms de fichier et permissions.
4. Importez les certificats générés dans les banques suivantes avec l'utilitaire Java keytool :
   - Certificats serveur et CA dans `server.keystore`
   - Certificat CA et client dans `server.truststore`
   - Certificat CA dans `ca.truststore`
   - Certificats client et CA dans `client.keystore`
   - Certificat CA et serveur dans `client.truststore`

> **REMARQUE :** L'utilitaire Java keytool se trouve sur Windows : `Program Files\Omniback\jre\bin` et sur UNIX : `/opt/omni/jre/bin`.

Remplacer le certificat CA

Pour remplacer le certificat CA existant, procédez comme suit :

1. Notez les permissions du fichier de certificat CA existant `cacert.pem`, situé dans :

   Windows

   `ProgramData\Omniback\Config\Server\certificates`

   UNIX

   `/etc/opt/omni/server/certificates`
2. Remplacez le fichier de certificat CA existant `cacert.pem` par le certificat CA généré.

Mettre à jour la chaîne de nom distinctif (DN)

Remplacez la chaîne de nom distinctif (DN) dans les fichiers `jce-webservice-roles.properties` et `dp-webservice-roles.properties` par la chaîne DN utilisée pour le certificat client. Ces fichiers se trouvent dans :

Windows

`ProgramData\Omniback\Config\Server\AppServer`

UNIX

`/etc/opt/omni/server/AppServer`

> **REMARQUE :** Dans la chaîne DN, ajoutez un backslash (\) avant les espaces et le caractère « = ».

Mettre à jour le fichier de configuration avec le mot de passe de la banque

Pour mettre à jour le fichier de configuration avec le mot de passe de la banque, procédez comme suit :

> **REMARQUE :** Cette tâche n'est requise que si les nouvelles banques sont créées avec un nouveau mot de passe.

1. Actualisez les fichiers de configuration webservice.properties et standalone.xml avec le mot de passe de la base de stockage tout en créant des fichiers de stockage, tels que `server.keystore`, `server.truststore`, `ca.truststore`, `client.keystore` et `client.truststore`.

   Les fichiers jde configuration sont situés dans :

   Windows

   •`ProgramData\OmniBack\Config\client\components\webservice.properties`

   •`ProgramData\OmniBack\Config\server\AppServer\standalone.xml`

   UNIX

   •`/etc/opt/omni/client/components/webservice.properties`

   • `/etc/opt/omni/server/AppServer/standalone.xml`

2. Dans le fichier `standalone.xml`, mettez à jour le mot de passe de banque (en gras) :

   ```
   <ssl name="ssl" password="M6.pOino06L3w" certificate-key-
   file="/etc/opt/omni/server/certificates/server/server.keystore" protocol="TLS"
   verify-client="want" ca-certificate-
   file="/etc/opt/omni/server/certificates/server/ca.truststore" ca-certificate-
   password="M6.pOino06L3w"/>
   ```

3. Dans le fichier `webservice.properties`, mettez à jour le mot de passe (en gras) :

   ```
    <jsse keystore-password="M6.pOino06L3w" keystore-
   url="/etc/opt/omni/server/certificates/server/server.keystore" truststore-
   password="M6.pOino06L3w" truststore-
   url="/etc/opt/omni/server/certificates/server/server.truststore"/>

   <jsse keystore-password="M6.pOino06L3w" keystore-
   url="/etc/opt/omni/server/certificates/server/server.keystore" truststore-
   password="M6.pOino06L3w" truststore-
   url="/etc/opt/omni/server/certificates/server/server.truststore"/>

    <ssl name="ssl" password="M6.pOino06L3w" certificate-key-
   file="/etc/opt/omni/server/certificates/server/server.keystore" protocol="TLS"
   verify-client="want" ca-certificate-
   file="/etc/opt/omni/server/certificates/server/ca.truststore" ca-certificate-
   password="M6.pOino06L3w"/>
   ```

Gestion des correctifs Data Protector

Les correctifs Data Protector sont fournis par le biais de assistance clientèle et peuvent être téléchargés sur le site en ligne de l'assistance logicielle : https://softwaresupport.softwaregrp.com/. Data Protector fournit des correctifs individuels et des paquets de correctifs.

Vérifier les correctifs Data Protector installés

Vous pouvez vérifier les correctifs Data Protector qui sont installés sur un système de la cellule. Pour vérifier les correctifs Data Protector installés sur un système spécifique d'une cellule, utilisez l'interface utilisateur graphique ou l'interface de ligne de commande Data Protector.

> **REMARQUE :**
> Après avoir installé un correctif spécifique pour un site ou un paquet de correctifs, celui-ci sera toujours répertorié dans le rapport des correctifs, même s'il a été par la suite inclus dans d'autres correctifs.

Conditions préalables

- Pour utiliser cette fonctionnalité, vous devez avoir installé le composant `User Interface`.

Limites

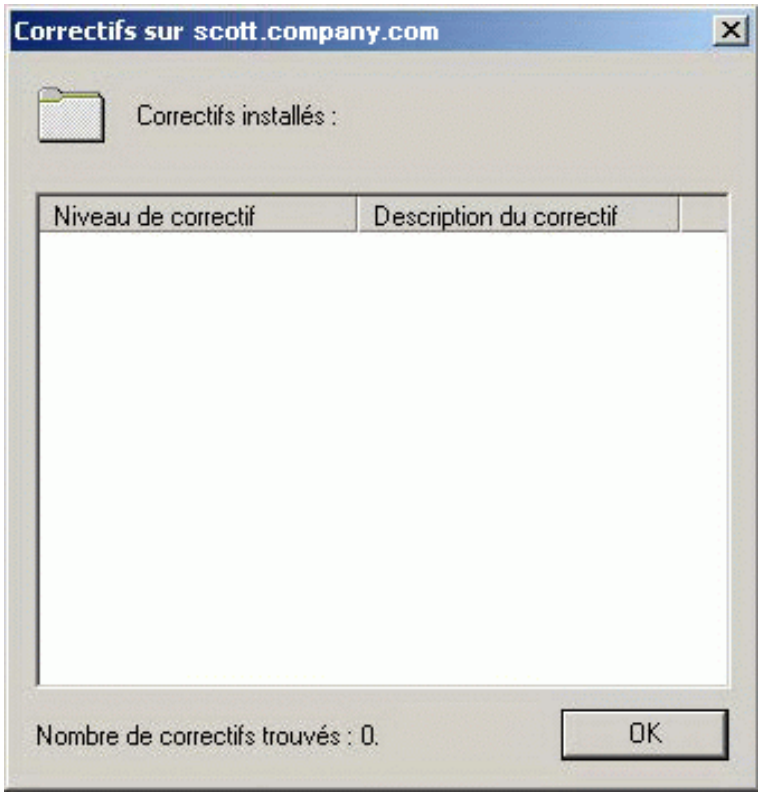
- La vérification du correctif permet uniquement de vérifier les correctifs qui sont installés sur les systèmes de la même cellule.

Vérifier les correctifs Data Protector à l'aide de l'interface utilisateur graphique

Pour vérifier les correctifs installés sur un client spécifique à l'aide de l'interface utilisateur graphique Data Protector

1. Dans la liste de contexte, sélectionnez **Clients**.
2. Dans la fenêtre de navigation, développez l'élément **Clients**, puis 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 appliqués**.

Vérifier les correctifs installés



Si des correctifs sont détectés sur le système, la procédure de vérification renvoie le niveau et la description de chaque correctif, 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 renvoie un message d'erreur.

4. Cliquez sur **OK** pour fermer la fenêtre.

Vérifier les correctifs Data Protector à l'aide de l'interface de ligne de commande

Pour vérifier les correctifs installés sur un client spécifique à l'aide de l'interface de ligne de commande Data Protector, exécutez la commande `omnicheck -patches -host` *`hostname`*, où *nom_hôte* est le nom du système à vérifier.

Pour plus d'informations sur la commande `omnicheck`, reportez-vous à la page man de `omnicheck`.

Correctifs requis par Data Protector

Pour les correctifs Data Protector, reportez-vous au site https://softwaresupport.softwaregrp.com/ pour obtenir les dernières informations.

Correctifs du système Windows

Pour les systèmes utilisant Windows, contactez l'entreprise Microsoft afin de télécharger le dernier Windows Service Pack de Microsoft.

Correctifs du système HP-UX

Pour obtenir les correctifs des systèmes exécutant les systèmes d'exploitation HP-UX, voir https://softwaresupport.softwaregrp.com/ pour plus d'informations ou pour obtenir les derniers correctifs. Installez les derniers correctifs avant de contacter le service d'assistance. Les correctifs répertoriés peuvent être remplacés par de nouveaux.

Micro Focus recommande d'installer régulièrement le package logiciel d'extension fourni pour HP-UX. Il s'agit d'un regroupement de correctifs recommandés, dont certains sont indiqués ci-dessous. Contactez le service d'assistance de clientèle pour obtenir la version actuelle du package logiciel d'extension HP-UX.

HP-UX 11.11

Les paquets de correctifs HP-UX 11.11 suivants sont requis par Data Protector :

Service pack	Nom du paquet	Description
Utilisez le dernier	GOLDQPK11i	Paquet actuel de correctifs pour HP-UX 11.11
Utilisez le dernier	HWEnable11i	Correctifs matériels requis

Les correctifs individuels HP-UX 11.11 suivants sont recommandés pour tous les systèmes de la cellule Data Protector :

Nom de correctif	Plate-forme matérielle	Description
PHCO_40310	s700, s800	correctif cumulatif libc
PHSS_41214	s700, s800	ld(1) et correctif cumulatif des outils associés
KRNG11i	s700, s800	Générateur de nombres aléatoires puissant

Les correctifs individuels HP-UX 11.11 suivants sont recommandés pour tous les clients HP-UX 11.11 de la cellule Data Protector :

Nom de correctif	Plate-forme matérielle	Description
Utilisez le dernier	s700, s800	Correctifs Serviceguard pour la version que vous utilisez

Le produit suivant et le correctif HP-UX 11.11 doivent être installés sur chaque système Agent de disque Data Protector à partir duquel les données seront sauvegardées sous forme cryptée AES 256-bit :

Numéro du produit ou nom du correctif	Plate-forme matérielle	Description
KRNG11I	s700, s800	Générateur de nombres aléatoires puissant HP-UX
PHKL_27750	s700, s800	activation vpar, activation krng

De plus, pour utiliser IPv6 sur HP-UX 11.11, le paquet suivant et les correctifs sont requis par Data Protector :

Nom du paquet ou du correctif	Plate-forme matérielle	Description
Paquet IPv6NCF11i ou les correctifs de transition TOUR	s700, s800	Correctif de transition de transport

HP-UX 11.23

Les paquets de correctifs HP-UX 11.23 suivants sont requis par Data Protector :

Service pack	Nom du paquet	Description
Utilisez le dernier	QPK1123	Paquet actuel de correctifs pour HP-UX 11.23

Les correctifs individuels HP-UX 11.23 suivants sont recommandés pour tous les clients HP-UX 11.23 de la cellule Data Protector :

Nom de correctif	Plate-forme matérielle	Description
PHKL_32272 [1]	s700, s800	Modifications pour résoudre les problèmes intermittents dans getacl/setacl.
PHSS_41178	s700, s800	correctif cumulatif liaisons et fdp

HP-UX 11.31

Les paquets de correctifs HP-UX 11.31 suivants sont requis par Data Protector :

Service pack	Nom du paquet	Description
Utilisez le dernier	QPK1131	Paquet actuel de correctifs pour HP-UX 11.31

Les correctifs individuels HP-UX 11.31 suivants sont requis par Data Protector :

[1] Ce correctif est requis pour prendre en charge la fonctionnalité de la liste de contrôle d'accès (ACL).

Nom de correctif	Plate-forme matérielle	Description
PHCO_38050	Itanium, PA-RISC	correctif cumulatif bibliothèque pthread
PHKL_38055	Itanium, PA-RISC	correctif cumulatif planificateur
PHSS_41179	Itanium, PA-RISC	correctif cumulatif liaisons et fdp

Correctifs du système SUSE Linux Enterprise Server

Utilisez les derniers correctifs recommandés du système, fournis par SUSE.

Correctifs du système Red Hat Enterprise Linux

Utilisez les derniers correctifs recommandés du système, fournis par Red Hat.

Installation des correctifs

Les correctifs Gestionnaire de cellule peuvent être installés localement. Toutefois, afin de corriger les clients, Serveur d'installation est requis. Après l'application du correctif sur Serveur d'installation, vous pouvez corriger les clients à distance.

> **IMPORTANT :**
> Sur les systèmes HP-UX, avant de corriger le Gestionnaire de cellule avec un correctif Gestionnaire de cellule (`CS`), arrêtez les services Data Protector à l'aide de la commande Data Protector `omnisv`, puis redémarrez-les après avoir terminé l'application du correctif.

Si les correctifs individuels sont inclus dans un paquet de correctifs, vous ne pouvez installer que le paquet dans son intégralité. Pour plus d'informations, reportez-vous aux instructions d'installation fournies avec le correctif.

Pour vérifier les correctifs installés sur le système, vous pouvez utiliser l'interface utilisateur graphique ou l'interface de ligne de commande Data Protector. Voir Vérifier les correctifs Data Protector installés, Page 226.

Installation de correctifs sur le Gestionnaire de cellule configuré sur Symantec Veritas Cluster Server

Lorsque vous installez un correctif pour des composants Gestionnaire de cellule (correctif CS et Patch Bundle), le correctif doit être appliqué localement sur chaque nœud d'abord. La procédure d'application de correctif pour le Gestionnaire de cellule de cluster s'exécutant sur Symantec Veritas Cluster Server est similaire à la mise à niveau (voir Mise à niveau du Gestionnaire de cellule configuré sur Symantec Veritas Cluster Server) avec les exceptions suivantes :

1. Les étapes de configuration doivent être ignorées (en d'autres termes, le `omniforsg.ksh` ne doit pas être exécuté.)
2. Les services Data Protector ne doivent pas être lancés avant l'installation du correctif.

Après l'installation locale des correctifs (si nécessaire), les composants non Gestionnaire de cellule et le composant principal doivent être mis à niveau à partir du serveur d'installation ayant fait l'objet du correctif. Il s'agit également de la procédure d'installation de correctif normale pour les Gestionnaire de cellule non cluster.

Installation et suppression des paquets de correctifs Data Protector

Si Data Protector est déjà installé sur votre système, vous pouvez également installer un paquet de correctifs Data Protector (un ensemble de correctifs Data Protector) sur ce système.

Pour installer un paquet de correctifs Data Protector sur les systèmes UNIX, vous pouvez utiliser le script `omnisetup.sh`. Sur les systèmes Windows, l'installation d'un paquet de correctifs est fournie en tant que fichier exécutable.

Vous pouvez également supprimer le paquet de correctifs. Après avoir supprimé le paquet de correctifs, la dernière version de Data Protector est conservée sur le système. Pour plus d'informations, reportez-vous aux instructions d'installation fournies avec le paquet de correctifs.

Installation et suppression de paquets de correctifs Data Protector sur des systèmes UNIX

Pour installer un paquet de correctifs Data Protector, utilisez la commande `omnisetup.sh` fournie dans l'archive tar en association avec les fichiers du paquet de correctifs. Utilisez l'option `-bundleadd`.

Abonnement à la télémétrie

Pour vous abonner à la collecte de données de télémétrie, acceptez la licence d'agrément de télémétrie et renseignez les détails demandés en utilisant l'option `omnisetup.sh` de la commande `-telemetry`.

Les options de la commande utilisées pour la télémétrie sont : `-compname`, `-proxyhost`, `-proxyport`, `-proxyuser`, `-proxypasswd`, `-no_telemetry`, et `-accept_obsolescence`.

Pour plus d'informations sur la commande `omnisetup.sh`, consultez le *Guide de référence de l'ILC Data Protector*.

> **REMARQUE :**
> L'abonnement à la télémétrie peut être configuré ultérieurement à l'aide de l'interface utilisateur graphique Data Protector, si ce n'est pas fait lors du processus d'installation.

Vous ne pouvez installer un paquet de correctifs Data Protector que sur le Serveur d'installation et le Gestionnaire de cellule. Si l'installation échoue ou si vous l'arrêtez, vous pouvez continuer l'installation et installer le reste des correctifs (pris en charge avec les systèmes Linux uniquement), annuler les correctifs installés et revenir au niveau des correctifs précédents, ou quitter l'installation sans installer tous les correctifs.

Pour supprimer le paquet de correctifs Data Protector, utilisez la commande `omnisetup.sh -bundlerem`.

Pour plus d'informations, reportez-vous aux instructions d'installation fournies avec le correctif ou le paquet de correctifs.

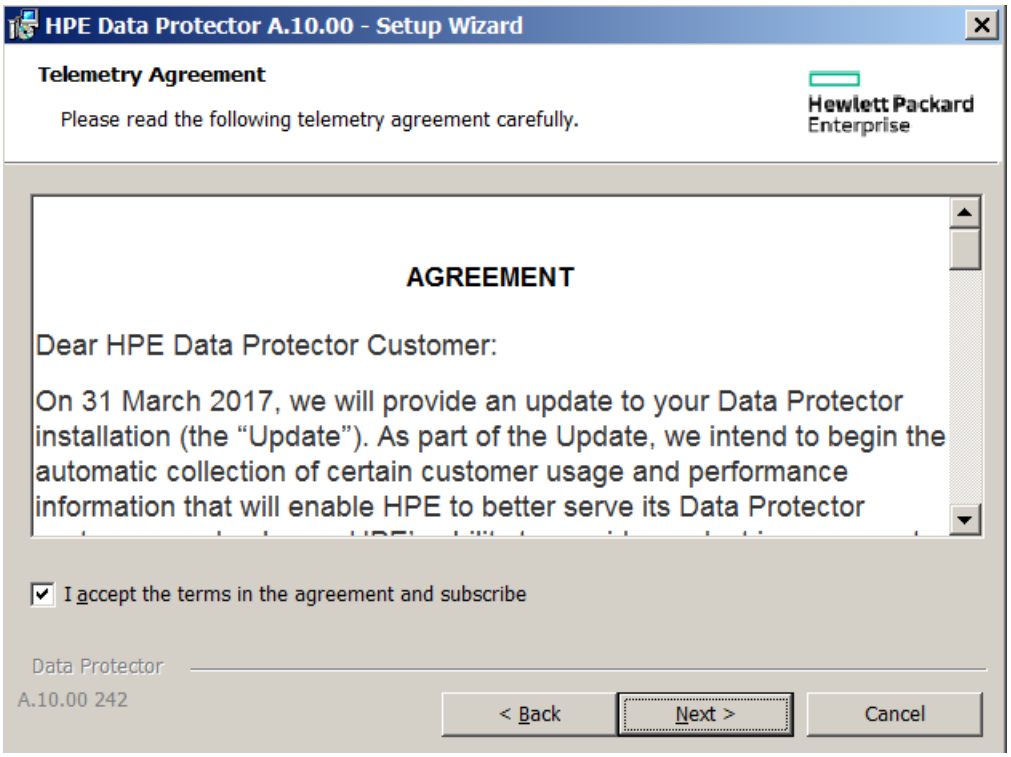
Installation et suppression des paquets de correctifs Data Protector sur les systèmes Windows

Un paquet de correctifs Data Protector pour Windows est fourni sous forme de fichier exécutable (par exemple, `DPWINBDL_00701.exe`). Vous pouvez installer un paquet de correctifs Data Protector sur le Serveur d'installation, le Gestionnaire de cellule ou sur le système client.

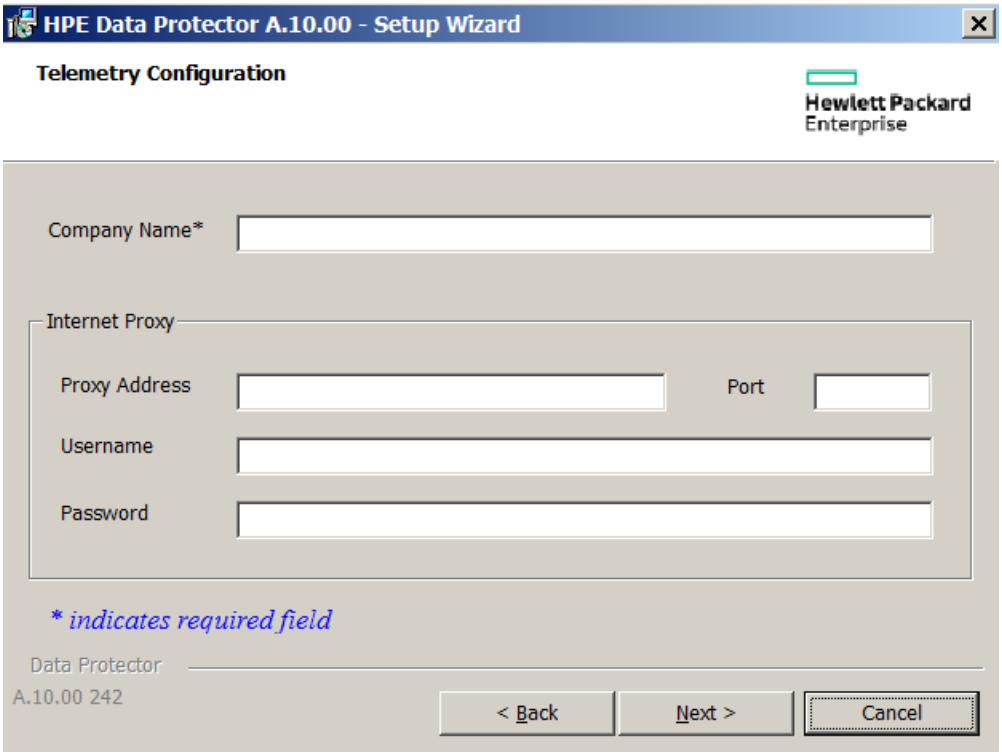
Pour installer le paquet de correctifs sur un système Windows, exécutez la commande *`BundleName`*`.exe`.

Abonnement à la télémétrie

- **Licence d'agrément de télémétrie** : Pour vous abonner à la collecte de données de télémétrie, acceptez la licence d'agrément de télémétrie et renseignez les détails demandés. Pour plus d'informations sur la télémétrie, consultez le *Guide de l'Administrateur Data Protector*.



- **Configuration de la télémétrie** : Après avoir accepté la licence d'agrément, il vous faut mettre à jour les paramètres suivants :



- Nom de la société : le nom de la société.
- Adresse proxy : l'adresse du serveur proxy.
- Port : le port du serveur proxy.
- Nom d'utilisateur : nom d'utilisateur de connexion au serveur proxy.
- Mot de passe : mot de passe associé au nom d'utilisateur.

> **REMARQUE :**
> Les configurations proxy sont nécessaires pour le chargement des données de télémétrie depuis le client de Console de cellule (CC) vers l'infrastructure Data Protector.

> **REMARQUE :**
> L'abonnement à la télémétrie peut être configuré ultérieurement à l'aide de l'interface utilisateur graphique Data Protector, si vous le refusez lors du processus d'installation.

La commande reconnaît les composants installés sur le système et les met à niveau vers le dernier correctif.

Pour supprimer le paquet de correctifs Data Protector, utilisez la commande `remove_patch.bat` située dans l'emplacement de commandes Data Protector par défaut dans le répertoire `utilns`.

`remove_patch`*BundleName**DPInstallationDepot* où *DPInstallationDepot* est l'emplacement à partir duquel Data Protector (non pas le paquet de correctifs) a été installé. Par exemple, pour supprimer le correctif Servicbundle `b701`, avec Data Protector installé à partir de `D:\WINDOWS_OTHER`, exécutez :

```
remove_patch.bat b701 D:\WINDOWS_OTHER
```

Vous pouvez supprimer un paquet de correctifs Data Protector du Serveur d'installation, du Gestionnaire de cellule ou du système client.

> **REMARQUE :**
> Sur les systèmes Windows, il est également possible de supprimer des correctifs individuels avec la commande `remove_patch.bat` Toutefois, assurez-vous de ne pas supprimer le correctif principal tant que d'autres correctifs individuels sont installés sur le système. Dans le cas contraire, vous ne pourrez pas supprimer d'autres correctifs individuels ultérieurement.
>
> Lorsque certains des composants Data Protector sont installés sur le système qui a été introduit après la version majeure, assurez-vous que le produit sur un tel système est remis à jour vers le niveau de correctif auquel ces composants sont connus ou supprimez ces composants avant de désinstaller le correctif principal ou les paquets de correctifs. Pour obtenir des informations sur la suppression des composants Data Protector, consultez la section Modification des composants logiciels Data Protector, Page 238.

Pour plus d'informations, reportez-vous aux instructions d'installation fournies avec le correctif ou le paquet de correctifs.

Mettre le correctif Internal Database à une version antérieure

Pour Data Protector 9.07 et versions supérieures, la base de données interne doit être mise à une version antérieure avant la suppression du correctif.

Pour mettre le correctif Internal Database à une version antérieure, procédez comme suit :

1. Arrêtez tous les services à l'exception de la base de données interne en exécutant les commandes suivantes :

   ```
   omnisv stop
   ```

   ```
   omnisv start -idb_only
   ```

2. Exécutez la mise à niveau de la base de données interne vers la version antérieure Data Protector 9.04 :

   Systèmes Windows :

   ```
   cd %DP_HOME_DIR%bin\dbscripts
   ```

   ```
   omnidbutil -run_script CPE\downgrade_to_904.sql
   ```

   Systèmes GNU/Linux ou UNIX :

   ```
   cd /opt/omni/sbin/dbscripts
   ```

   ```
   omnidbutil -run_script CPE/downgrade_to_904.sql
   ```

3. Procédez à la suppression du correctif et supprimez tous les correctifs jusqu'à ce que la version Data Protector puisse être mise à niveau vers une version antérieure à la version DP 9.04.
4. Ré-effectuez une mise à niveau vers la version 9.04 au minimum ou une version supérieure immédiatement après la suppression du correctif et avant d'exécuter la sauvegarde ou la restauration.

Gestion des correctifs spécifiques au site et des correctifs logiciels

Les correctifs spécifiques au site (SSP) et les correctifs logiciels (HF) sont appliqués manuellement sur les clients ou les gestionnaires cellule concernés.

Préparation du serveur d'installation pour une installation distante de correctifs SSP et de modules TM

Les packages Data Protector SSP ou HF sont fournis par le service assistance clientèle. Vous devez copier le package SSP ou HF dans l'entrepôt du serveur d'installation à l'emplacement suivant :

UNIX : `/opt/omni/databases/vendor/ssphf`

Windows : `Data_Protector_program_data\depot\ssphf` (Par exemple : `C:\ProgramData\Omniback\depot\ssphf`)

> **REMARQUE :**
> Les correctifs logiciels sont livrés sous forme de fichiers ZIP. Vous devez décompresser les packages SSP ou HF avant de commencer à utiliser les fichiers sur le serveur d'installation. Sous Windows, vous pouvez copier le fichier zip extrait dans `Data_Protector_program_data\depot\ssphf`. Sous Linux/UNIX, vous devez décompresser le fichier tar.gz extrait (en utilisant gzip) sur le système Linux/UNIX après avoir copié le package SSP ou HF sur le serveur d'installation. Le format attendu du package SSP ou HF sur le serveur d'installation est ZIP pour Windows et TAR pour Linux/UNIX.

Pour vérifier les packages SSP/HF disponibles pour une installation distante sur le serveur d'installation, procédez comme suit :

1. Dans la liste de contexte, sélectionnez **Clients**.
2. Dans la fenêtre de navigation, développez l'élément **Serveurs d'installation**, puis sélectionnez un système de la cellule pour lequel vous souhaitez contrôler les modules SSP/HF.
3. Dans la zone Résultats, cliquez sur **SSP et HF...** pour ouvrir la fenêtre contextuelle des modules SSP/HF.

   Si des modules SSP/HF se trouvent sur le système, vous obtenez afficher l'ID du module SSP ou HF, ainsi que le nombre de ces modules présents sur le serveur d'installation.
4. Cliquez sur **OK** pour fermer la fenêtre.

Installation de correctifs spécifiques au site ou de correctifs logiciels sur les clients

Une fois le package SSP/HF copié sur le serveur d'installation, vous pouvez sélectionner le module SSP/HF en vue de l'installation en utilisant la liste de sélection des modules SSP/HF disponible dans l'interface graphique de Data Protector. Si le module SSP/HF est sélectionné, tous les autres composants de Data Protector sont désactivés pour la sélection, car un seul module SSP/HF peut être

installé à la fois. Le module SSP/HF pouvant fournir des fichiers binaires pour différents composants de Data Protector, seuls les fichiers binaires des composants Data Protector installés seront appliqués sur le système. Toutefois, le statut du package SSP/HF est toujours affiché comme étant installé, puisque comme tous les fichiers binaires applicables sont appliqués sur le système.

> **REMARQUE :**
> L'installation à distance des packages SSP/HF est également disponible dans MoM-GUI.

L'installation à distance du package SSP/HF consiste à déployer le package SSP/HF sur le système distant, à l'extraire, puis à copier les fichiers binaires applicables vers leur emplacement cible. En tant que telle, cette opération ne traite pas les procédures spéciales nécessaires pour remplacer les fichiers en cours d'utilisation.

Pour installer manuellement le module SSP/HF sur les clients, procédez comme suit :

- Copiez le package d'archives SSP/HF sur l'hôte de destination et procédez à son extraction.
- Arrêtez les services Data Protector. Seuls les services ou les processus affectés peuvent être arrêtés.
- Appliquez les fichiers binaires SSP/HF comme suit :
  - Copiez les fichiers depuis package SSP/HF extrait vers l'emplacement cible applicable. (Copiez uniquement les fichiers pour lesquels les composants Data Protector sont installés).
  - Copiez le `CII_<SSPHFNAME>` à l'emplacement correspondant.

    Par exemple :

    Windows : `Data_Protector_program_data\config\Client\ssphf`

    Autres plates-formes : `\etc\opt\omni\client\ssphf`

Vous pouvez également installer le package SSP/HF sur les clients à l'aide de la commande `ob2install`. Pour plus d'informations sur la commande `ob2install`, reportez-vous à la page man de `ob2install`.

Dans la plupart des cas, vous devez installer manuellement les packages SSP/HF, qui fournissent certains des fichiers binaires répertoriés :

- Fichiers binaires du serveur de cellule (concernant notamment les gestionnaires de services et de sessions).
- Fichiers binaires CORE - **Windows :** fichiers binaires de services et messages de catalogue `Inet`. Par exemple, `OmniInet.exe`, `OmniEnu.dll`, etc.
- Fichiers binaires d'interface graphique : lorsque vous utilisez l'interface GUI de Data Protector sur l'hôte auquel ce module SSP/HF doit être appliqué.

> **REMARQUE :**
> L'ajout de composants à un gestionnaire de cellule compatible cluster exécuté sur MS Cluster Server est désactivé, car ces modules SSP/HF ne sont pas installables à distance et doivent être appliqués manuellement sur tous les nœuds de cluster applicables.

Rétablissement des fichiers binaires remplacés par SSP/HF

Au cours de l'installation à distance des fichiers binaires SSP/HF, les fichiers en cours sont sauvegardés et laissés sur le système en vue de leur utilisation ultérieure.

Par exemple,

Windows : `Data_Protector_program_data\tmp\ssphf\<SSPHFNAME>\<DATE_TIME>`

Autre plate-forme : . `/var/opt/omni/tmp/ssphf/<SSPHFNAME>/<DATE_TIME>`. (L'emplacement exact dépend de la plateforme).

Pour rétablir les fichiers binaires remplacés par l'installation SSP/HF en mode Push, envisagez l'une des approches suivantes :

- Rétablissez manuellement les fichiers binaires sauvegardés.
- Réinstallez les composants affectés sur le système. (Option préférable)
- Mettez le système à niveau à partir de l'interface utilisateur graphique de Data Protector. (Contexte des **clients**)
- Exécutez l'opération de réparation à partir de l'assistant de configuration Data Protector. (Applicable aux systèmes Windows uniquement)
- Installez un autre package SSP/HF quelconque contenant tous les fichiers binaires inclus dans le cadre de l'ancien module SSP/HF à remplacer.

Chaque opération Push du module SSP/HF génère son propre fichier journal à l'emplacement suivant, pour les besoins du dépannage des opérations ayant échoué :

Windows : `Data_Protector_program_data\log\ssphf_install_<DATE_TIME>.log`

Unix : `/var/opt/omni/log/ssphf_install_<PID>.log` (L'emplacement exact dépend de la plate-forme)

Vérification des modules SSP ou HF installés

Vous pouvez vérifier quels correctifs spécifiques au site ou correctifs logiciels de Data Protector sont installés sur un système dans la cellule en utilisant l'interface utilisateur graphique ou la ligne de commande de Data Protector.

> **REMARQUE :**
> Après une installation réussie d'un module SSP/HF, les instances correspondantes affichent l'état d'installation `Installed`. En cas de défaillance, les fichiers binaires sont rétablis et les statuts de ces modules SSP/HF ne sont pas répertoriés.

L'installation à distance du module SSP/HF installe uniquement les fichiers binaires des composants qui sont installés sur l'hôte cible. Le package SSP/HF peut afficher l'un des statuts suivants :

- Installé : tous les fichiers binaires SSP/HF des composants Data Protector installés sur le système sont copiés.
- Partiellement : quelques fichiers binaires du module SSP/HF pour les composants Data Protector installés sur le système ne sont pas installés. Cette situation peut se produire pour deux raisons :

1. Si un package SSP/HF complet est installé, son statut est indiqué comme `Installed`. En revanche, à un moment donné, si un autre composant SSP/HF ou Data Protector issu de l'installation initiale est poussé vers le système en remplaçant certains des fichiers binaires fournis par le module SSP/HF, le statut d'un tel module sera modifié sur `Partly` installé.
2. Si le package SSP/HF fournit des fichiers binaires pour plusieurs composants Data Protector (exemple : `da` et `ma`) et si seulement quelques composants sont installés sur le système (par exemple : `da`), seuls les fichiers binaires pour les composants installés seront appliqués au

système (autrement dit, `da`). Le statut d'installation d'un tel package sera indiqué comme `Installed`. Si, plus tard, le composant `ma` est installé sur le système, le statut du package sera remplacé par `Partly` installé.

> **REMARQUE :**
> Si tous les fichiers binaires installés par le package SSP/HF sont remplacés par certains autres fichiers binaires, un tel package SSP/HF sera traité comme n'étant plus installé et il ne s'affichera pas dans la liste des statuts SSP/HF.

Pour afficher la liste des fichiers binaires SSP/HF qui ont été modifiés, procédez comme suit :

- Exécutez le service `Inet` avec l'option de débogage.
- Vérifiez les statuts des packages SSP/HF installés.
- Consultez le fichier journal `Inet` pour voir quels fichiers binaires ont été modifiés.

Vérification des packages SSP ou HF à l'aide de l'interface graphique

Pour vérifier quels packages SSP/HF sont installés sur un client particulier à l'aide de l'interface utilisateur graphique de Data Protector :

1. Dans la liste de contexte, sélectionnez **Clients**.
2. Dans la fenêtre de navigation, développez l'élément **Clients**, puis sélectionnez un système de la cellule pour lequel vous souhaitez contrôler les packages SSP/HF installés.
3. Dans la zone Résultats, cliquez sur **SSP et HF...** pour ouvrir la fenêtre contextuelle des modules SSP/HF.

   Si des packages SSP/HF ont été détectés sur le système, la vérification renvoie l'identifiant et le statut de chaque instance SSP/HF, ainsi que le nombre de SSP/HF installés.
4. Cliquez sur **OK** pour fermer la fenêtre.

Vérification des packages SSP ou HF à l'aide d'une ligne de commande

Pour vérifier quels packages SSP/HF sont installés sur un client particulier à l'aide de la ligne de commande de Data Protector, exécutez la commande `omnicheck -ssphf -host` *`hostname`*, où *hostname* désigne le nom du système à vérifier.

Pour plus d'informations sur la commande `omnicheck`, reportez-vous à la page man de `omnicheck`.

Modification des composants logiciels Data Protector

Cette section décrit la procédure permettant de supprimer et d'ajouter des composants logiciels Data Protector depuis ou vers les systèmes Windows, HP-UX, Solaris et Linux. Pour la liste des composants Data Protector pris en charge pour un système d'exploitation particulier, consultez les Annonces sur les produits, notes sur les logiciels et références Data Protector.

Des composants logiciels Data Protector peuvent être ajoutés au Gestionnaire de cellule ou sur un client en utilisant l'interface utilisateur graphique Data Protector. Vous effectuez l'installation à distance des composants sélectionnés en utilisant la fonctionnalité Serveur d'installation. Pour connaître la procédure détaillée, voir Installation à distance, Page 95.

Les composants Data Protector peuvent être supprimés localement sur le Gestionnaire de cellule, un Serveur d'installation ou un client.

Sur les systèmes Windows

Pour ajouter ou supprimer des composants logiciels Data Protector sur un système Windows.

Cette procédure est uniquement possible si le dépôt d'installation avec le même niveau de correctif est disponible. Dans certains cas, le chemin d'accès au dépôt d'installation doit être défini, par exemple :**\\<DP_IS_SYSTEM>\Omniback\x8664**.

1. Dans le Panneau de configuration de Windows, cliquez sur **Ajout/Suppression de programmes / Programmes et fonctionnalités**.
2. Sélectionnez **Data Protector 10.00** et cliquez sur **Modifier**.
3. Cliquez sur **Suivant**.
4. Dans la fenêtre Maintenance du programme, cliquez sur **Modifier** puis sur **Suivant**.
5. Dans la fenêtre Installation personnalisée, sélectionnez les composants que vous voulez ajouter et/ou désélectionnez les composants logiciels que vous voulez supprimer. Cliquez sur **Suivant**.
6. Cliquez sur **Installer** pour démarrer l'installation ou la suppression des composants logiciels.
7. Une fois l'installation terminée, cliquez sur **Terminer**.

Clients compatibles cluster

Si vous modifiez les composants logiciels Data Protector sur les clients compatibles cluster, l'opération doit être réalisée localement, à partir du package d'installation, sur chaque nœud cluster. Ensuite, vous devez importer manuellement le nom d'hôte du serveur virtuel dans la cellule Data Protector en utilisant l'interface utilisateur graphique.

Sur les systèmes HP-UX

Vous pouvez ajouter de nouveaux composants en utilisant la fonctionnalité Serveur d'installation.

Pour supprimer des composants, utilisez la commande `swremove`.

Procédure

Pour supprimer des composants logiciels Data Protector

1. Connectez-vous en tant que `root`, puis exécutez la commande `swremove`.
2. Double-cliquez sur **B6960MA**, **DATA-PROTECTOR** puis sur **OB2-CM** pour afficher une liste de composants Data Protector.

3. Sélectionnez les composants à supprimer.
4. Dans le menu **Actions**, cliquez sur **Marquer pour suppression** pour marquer les composants que vous souhaitez supprimer.
5. Quand les composants que vous souhaitez supprimer sont marqués, cliquez sur **Supprimer** dans le menu **Actions**, puis cliquez sur **OK**.

> **REMARQUE :**
> Lorsque vous marquez des composants Data Protector dont la suppression peut empêcher les composants restants de fonctionner correctement, la **boîte de dialogue Message de dépendance** apparaît avec la liste des composants dépendants.

Spécificités du Serveur 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 la suppression de l'intégration. Pour plus d'informations, voir *Guide d'intégration Data Protector*.

Sur les systèmes Linux

Vous pouvez ajouter de nouveaux composants en utilisant la fonctionnalité Serveur d'installation. Sur les systèmes Linux, certains composants Data Protector sont interdépendants et ne peuvent fonctionner correctement si l'un d'eux est supprimé. Le tableau ci-dessous affiche les composants et leurs interdépendances.

Dépendances des composants logiciels **Data Protector sur Linux**

Composants	Dépend de
Gestionnaire de cellule	
OB2-CC, OB2-DA, OB2-MA, OB2-DOCS	OB2-CORE, OB2-TS-CORE
OB2-CS	OB2-CORE, OB2-TS-CORE, OB2-CC
OB2-TS-CS, OB2-TS-JRE, OB2-TS-AS, OB2-WS, OB2-JCE-DISPATCHER, OB2-JCE-SERVICEREGISTRY	OB2-CORE, OB2-TS-CORE, OB2-CC
Serveur d'installation	
OB2-CORE-IS	OB2-CORE
OB2-CF-P, OB2-TS-CFP	OB2-CORE-IS
OB2-CCP, OB2-DAP, OB2-MAP, OB2-NDMPP, OB2-AUTODRP, OB2-DOCSP, OB2-CHSP, OB2-FRAP,	OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP

Composants	Dépend de
OB2-JPNP, OB2-INTEGP, OB2-VMWP, OB2-VMWAREGRE-AGENTP, OB2-SODAP, OB2-TS-PEGP	
OB2-DB2P OB2-EMCP OB2-INFP OB2-LOTP OB2-OR8P OB2-SAPDP OB2-SAPP OB2-SSEAP OB2-SYBP	OB2-INTEGP, OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP
OB2-SMISP	OB2-CORE-IS, OB2-CF-P, OB2-TS-CFP, OB2-TS-PEG-P

Procédure

Pour supprimer des composants Data Protector des systèmes Linux

1. Assurez-vous d'avoir terminé toutes les sessions Data Protector et d'avoir quitté l'interface utilisateur graphique.
2. Saisissez la commande `rpm | grep OB2` pour répertorier tous les composants Data Protector installés.
3. Dans l'ordre inverse de la séquence d'installation, supprimez les composants mentionnés au cours de l'étape 2 en utilisant la commande `rpm -e package name` et en répondant aux invites.

Sur d'autres systèmes UNIX

Lors de la suppression manuelle de composants d'un client Data Protector sur un système UNIX autre que HP-UX ou Linux, actualisez le fichier `omni_info` dans `/usr/omni/bin/install`.

Pour chacun des composants supprimés, supprimez la chaîne de version du composant associée du fichier `omni_info`.

Si vous supprimez uniquement les composants d'un client Data Protector et que vous n'avez pas exporté le client de la cellule, vous devrez actualiser la configuration de cellule dans le fichier `cell_info` (au niveau du Gestionnaire de cellule). Cela peut être effectué en exécutant la commande suivante sur un système de la cellule avec la console de cellule installée :

`omnicc -update_host HostName`

Vérification de l'installation

Pour contrôler si les composants logiciels Data Protector sont en cours d'exécution sur le Gestionnaire de cellule ou sur les systèmes client, vous pouvez vérifier l'installation à l'aide de l'interface utilisateur graphique Data Protector.

Conditions préalables

Vous devez disposer du serveur d'installation correspondant au type de système client (système UNIX ou système Windows) que vous utilisez.

Procédure

1. Dans la liste de contexte, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, développez l'élément **Clients**, cliquez avec le bouton droit de la souris sur le Gestionnaire de cellule ou le système client, puis cliquez sur **Vérifier installation** pour ouvrir l'assistant.
3. La liste de tous les systèmes client du même type (systèmes UNIX ou systèmes Windows) s'affiche. Sélectionnez les clients dont vous souhaitez vérifier l'installation, puis cliquez sur **Terminer** pour démarrer la vérification.

Les résultats de la vérification s'affichent dans la fenêtre Vérifier installation.

Désinstallation du logiciel Data Protector

Si la configuration de votre système change, vous souhaiterez peut-être désinstaller le logiciel Data Protector du système ou supprimer certains de ses composants logiciels.

La désinstallation consiste à supprimer du système tous les composants logiciels de Data Protector, y compris *toutes* les références à ce système dans l'IDB dans l'ordinateur 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. Pour supprimer les données de configuration après la désinstallation du logiciel Data Protector, supprimez les répertoires dans lesquels Data Protector a été installé.

Si d'autres données sont présentes dans le répertoire d'installation de Data Protector, assurez-vous d'avoir copié ces données vers un autre emplacement avant de désinstaller Data Protector. Dans le cas contraire, les données seront supprimées au cours du processus de désinstallation.

La désinstallation du logiciel Data Protector d'une cellule comprend les étapes suivantes :

1. Désinstallation du logiciel client Data Protector à l'aide de l'interface utilisateur graphique. VoirDésinstallation d’un client Data Protector, Page suivante.
2. Désinstallation de Data Protector Gestionnaire de cellule et Serveur d'installation. Voir Désinstallation du Gestionnaire de cellule et Serveur d'installation, Page 244.

Vous pouvez également désinstaller les composants logiciels Data Protector sans désinstaller le Gestionnaire de cellule ou le client. Voir Modification des composants logiciels Data Protector, Page 238.

Sur UNIX, vous pouvez également supprimer manuellement le logiciel Data Protector. Voir Suppression manuelle du logiciel Data Protector sur UNIX, Page 251.

Conditions préalables

Avant de désinstaller le logiciel Data Protector d'un ordinateur, vérifiez ce qui suit :

- Vérifiez que toutes les références à l'ordinateur sont 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. Pour plus d'informations sur la manière de modifier les spécifications de sauvegarde, consultez l'index *Aide de Data Protector* : "modification, spécifications de sauvegarde".
- Assurez-vous qu'aucun périphérique de sauvegarde ou baie de disques n'est connecté ou configuré sur le système que vous voulez désinstaller. Lorsque le système est exporté, Data Protector ne peut plus utiliser ses périphériques de sauvegarde ou ses baies de disques dans la cellule originale.
- Avant de procéder à la désinstallation, assurez-vous que toutes les requêtes GRE Power On sont fermées. De plus, assurez-vous que les sessions Migration en direct en cours d'exécution sont terminées ou annulées.

Désinstallation d'un client Data Protector

> **REMARQUE :**
> La procédure de désinstallation à distance requiert l'installation de Serveur d'installation pour les plateformes à partir desquelles vous désinstallez le logiciel Data Protector.

Pour désinstaller un client à distance sur l'interface utilisateur graphique Data Protector

1. Dans la liste de contexte, passez au contexte **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**. Il vous sera demandé si vous souhaitez également désinstaller le logiciel Data Protector.
3. Cliquez sur **Oui** pour désinstaller tous les composants logiciels du client, puis cliquez 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. Pour supprimer les données de configuration, supprimez les répertoires dans lesquels Data Protector a été installé.

Désinstallation des clients cluster

Si votre environnement Data Protector comporte des clients compatibles cluster et que vous souhaitez les désinstaller, vous devez effectuer l'opération localement. La procédure est identique à celle de désinstallation de Gestionnaire de cellule ou Serveur d'installation. Voir Désinstallation du Gestionnaire de cellule et Serveur d'installation, Page suivante.

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 les clients TruCluster, exportez tout d'abord le nœud virtuel. Désinstallez ensuite les clients Data Protector du/des nœud(s).

Clients HP OpenVMS

Un client OpenVMS Data Protector ne peut pas être supprimé à distance à l'aide d'un Serveur d'installation. Il doit être désinstallé localement.

Pour désinstaller un client Data Protector d'un système OpenVMS

1. Exportez tout d'abord le client concerné de la cellule Data Protector à l'aide de l'interface utilisateur graphique Data Protector, comme décrit dans Exportation de clients d'une cellule, Page 198.

   À la question demandant si vous souhaitez désinstaller également le logiciel Data Protector, répondez **Non**.
2. Pour supprimer le logiciel existant du 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 `YES`.

   > **IMPORTANT :**
   > Cela arrêtera le service Data Protector et supprimera tous les répertoires, fichiers et comptes associés à Data Protector sur le système OpenVMS.

Désinstallation du Gestionnaire de cellule et Serveur d'installation

Cette section décrit la procédure de désinstallation du Data Protector Gestionnaire de cellule et du logiciel Serveur d'installation des systèmes Windows, HP-UX et Linux.

Désinstallation des systèmes Windows

Désinstallation d'un cluster de serveur Microsoft

Pour désinstaller le logiciel Data Protector d'un système Windows

1. Assurez-vous d'avoir terminé toutes les sessions Data Protector et d'avoir quitté l'interface.
2. Dans le Panneau de configuration de Windows, cliquez sur **Ajout/Suppression de programmes**.
3. Selon que vous souhaitiez ou non laisser les données de configuration sur le système, différentes actions s'appliquent :

   > **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 Gestionnaire de cellule 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 désinstaller Data Protector et laisser les données de configuration Data Protector sur le système, sélectionnez **Data Protector 10.00** et cliquez sur **Supprimer**.
- Pour désinstaller Data Protector et supprimer les données de configuration de Data Protector, sélectionnez **Data Protector10.00**, cliquez sur **Modifier** 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.

Désinstallation des systèmes HP-UX

Le Gestionnaire de cellule pour HP-UX est toujours installé localement, en utilisant la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé localement, en utilisant l'utilitaire `swremove`.

> **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 Gestionnaire de cellule à celle qui était installée, notez que les données de configuration ne seront pas compatibles.
>
> Pour l'installation réussie d'une version antérieure, supprimez les répertoires Data Protector restants sur votre système après la désinstallation.

Conditions préalables

- Supprimez tout paquet de correctifs Data Protector installé avec la commande `omnisetup.sh -bundlerem`. Voir Installation et suppression de paquets de correctifs Data Protector sur des systèmes UNIX, Page 231.

Procédure

Avant de commencer à désinstaller le logiciel Data Protector, arrêtez les processus Data Protector en cours d'exécution sur le système Gestionnaire de cellule et/ou Serveur d'installation :

1. Connectez-vous en tant que root puis exécutez la commande `omnisv -stop`.
2. Saisissez la commande `ps -ef | grep omni` pour vérifier si tous les processus ont bien été arrêtés. Aucun processus Data Protector ne doit s'afficher après l'exécution de `ps -ef | grep omni`.

   Si des processus Data Protector sont encore en cours d'exécution, vous devez les arrêter à l'aide de la commande `kill` *`process_ID`* avant de procéder à la désinstallation.
3. Lancez `/usr/sbin/swremove DATA-PROTECTOR` pour désinstaller le logiciel Data Protector.

Pour supprimer de votre système les répertoires Data Protector restants, consultez Suppression manuelle du logiciel Data Protector sur UNIX, Page 251.

Désinstallation du Gestionnaire de cellule et/ou Serveur d'installation configuré sur Serviceguard

Si votre Gestionnaire de cellule et/ou Serveur d'installation est configuré sur un cluster Serviceguard, effectuez les étapes suivantes pour désinstaller le logiciel.

Nœud primaire

Connectez-vous au nœud principal et procédez aux étapes suivantes :

1. Arrêtez le package Data Protector :

   `cmhaltpkg PackageName`

   où *PackageName* correspond au nom du package cluster.

   Par exemple :

   `cmhaltpkg ob2cl`
2. Désactivez le mode cluster pour le groupe de volumes :

   `vgchange -c n vg_name`

   (où *vg_name* est le nom du chemin d'accès du groupe de volumes situé 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 vg_name`

   Par exemple :

   `vgchange -a y -q y /dev/vg_ob2cm`
4. Monter le volume logique sur le disque partagé :

   `mount lv_path shared_disk`

   (où *lv_path* est le nom du chemin d'accès du volume logique et *shared_disk* le point de montage ou répertoire partagé).

   Par exemple :

   `mount /dev/vg_ob2cm/lv_ob2cm /omni_shared`
5. Supprimez Data Protector en utilisant l'utilitaire 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 avec son contenu :

   `rm -rf /opt/omni`
9. Démonter le disque partagé :

umount *shared_disk*

Par exemple :

umount /omni_shared

10. Désactiver le groupe de volumes :

    vgchange -a n *vg_name*

    Par exemple :

    vgchange -a n /dev/vg_ob2cm

Nœud secondaire

Connectez-vous au nœud secondaire et procédez aux étapes suivantes :

1. Activez le groupe de volumes :

   vgchange -a y *vg_name*
2. Montez le disque partagé :

   mount *lv_pathshared_disk*
3. Supprimez Data Protector en utilisant l'utilitaire 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 avec son contenu :

   rm -rf /opt/omni
7. Supprimez les répertoires dans le système de fichiers partagé :

   rm -rf *shared_disk*/etc_opt_omni

   rm -rf *shared_disk*/var_opt_omni

   Par exemple :

   rm -rf /omni_shared/etc_opt_omni

   rm -rf /omni_shared/etc_opt_omni
8. Démonter le disque partagé :

   umount*shared_disk*
9. Désactiver le groupe de volumes :

   vgchange -a n *vg_name*

Data Protector a été entièrement supprimé du système.

Désinstaller le Gestionnaire de cellule et/ou Serveur d'installation configuré sur Symantec Veritas Cluster Server

Si votre Gestionnaire de cellule et/ou Serveur d'installation est configuré sur un Symantec Veritas Cluster Server, effectuez les étapes suivantes pour désinstaller le logiciel.

Nœud primaire

Connectez-vous au nœud principal et procédez aux étapes suivantes :

1. Mettez la ressource d'application Data Protector hors ligne.
2. Désactiver la ressource d'application Data Protector.
3. Désinstallez Data Protector.
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 avec son contenu :

   ```
   rm -rf /opt/omni
   ```

Nœud secondaire

Connectez-vous au nœud secondaire et procédez aux étapes suivantes :

1. Faites basculer le groupe de services Data Protector sur le nœud secondaire.
2. Désinstallez Data Protector.
3. Supprimez les liens programmables :

   ```
   rm /etc/opt/omni
   rm /var/opt/omni
   ```
4. Supprimez les répertoires de sauvegarde :

   ```
   rm -rf /etc/opt/omni.save
   rm -rf /var/opt/omni.save
   ```
5. Supprimez le répertoire Data Protector avec son contenu :

   ```
   rm -rf /opt/omni
   ```
6. Supprimez les répertoires dans le système de fichiers partagé :

   ```
   rm -rf shared_disk/etc_opt_omni
   rm -rf shared_disk/var_opt_omni
   ```

   Par exemple :

   ```
   rm -rf /omni_shared/etc_opt_omni
   rm -rf /omni_shared/var_opt_omni
   ```

Data Protector a été entièrement supprimé du système.

Désinstallation des systèmes Linux

Conditions préalables

- Supprimez tout paquet de correctifs Data Protector installé avec la commande `omnisetup.sh -bundlerem`. Voir Installation et suppression de paquets de correctifs Data Protector sur des systèmes UNIX, Page 231.

Gestionnaire de cellule

Le Gestionnaire de cellule pour Linux est toujours installé localement, en utilisant la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé localement, en utilisant 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 Gestionnaire de cellule à celle qui était installée, notez que les données de configuration ne seront pas compatibles.
>
> Pour l'installation réussie d'une version antérieure, supprimez les répertoires Data Protector restants sur votre système après la désinstallation.

Pour désinstaller Data Protector Gestionnaire de cellule, procédez comme suit :

1. Assurez-vous d'avoir terminé toutes les sessions Data Protector et d'avoir quitté l'interface utilisateur graphique.
2. Saisissez la commande `rpm -qa | grep OB2` pour répertorier tous les composants Data Protector installés sur le Gestionnaire de cellule.

   Les composants associés au Gestionnaire de cellule sont les suivants :

OB2-CORE	Logiciel central de Data Protector
OB2-TS-CORE	Bibliothèques des composants technologiques centraux de Data Protector
OB2-CC	Client de la console de cellule. Contient l'interface en ligne de commande.
OB2-TS-CS	Bibliothèques Pile technologique de Gestionnaire de cellule
OB2-TS-JRE	Environnement Java Runtime à utiliser avec Data Protector.
OB2-TS-AS	Serveur d'application de Data Protector
OB2-WS	Services web de Data Protector
OB2-JCE-DISPATCHER	Système de déploiement du moteur de contrôle de tâches
OB2-JCE-SERVICEREGISTRY	Registre de service du moteur de contrôle de tâches

OB2-CS	Logiciel Gestionnaire de cellule
OB2-DA	Client Agent de disque. Requis, sans quoi il est impossible de sauvegarder l'IDB.
OB2-MA	Client agent général de support Nécessaire pour attacher un périphérique de sauvegarde au Gestionnaire de cellule.
OB2-DOCS	Le sous-produit de documentation Data Protector qui inclut les guides Data Protector au format PDF et le *Aide de Data Protector* au format WebHelp.

Si des clients Data Protector ou un Serveur d'installation sont également installés sur le système, d'autres composants seront également listés.

> **REMARQUE :**
> Pour conserver l'installation d'autres composants de Data Protector, vous devez conserver le composant OB2-CORE car il est interdépendant des autres composants.

3. Dans l'ordre inverse de la séquence d'installation, supprimez les composants mentionnés au cours de l'étape précédente en utilisant la commande `rpm -e` *`package name`* et en répondant aux invites.

Serveur d'installation

Le Serveur d'installation pour UNIX sous Linux est toujours installé localement, en utilisant la commande `omnisetup.sh`. Par conséquent, il doit être désinstallé localement, en utilisant l'utilitaire `rpm`.

Pour désinstaller Data Protector Serveur d'installation, procédez comme suit :

1. Assurez-vous d'avoir terminé toutes les sessions Data Protector et d'avoir quitté l'interface.
2. Exécutez la commande `rpm -qa | grep OB2` pour répertorier tous les composants Data Protector et supprimer les packages d'installation de composants et à distance stockés sur le système Serveur d'installation.

   Les composants et les packages d'installation à distance associés au Serveur d'installation sont les suivants :

OB2-CORE	Client central de Data Protector. Veuillez noter qu'il est déjà installé si vous installez le Serveur d'installation sur le système du Gestionnaire de cellule.
OB2-TS-CORE	Bibliothèques des composants technologiques centraux de Data Protector.
OB2-CORE-IS	Client central de Serveur d'installation.
OB2-CFP	Client central commun du Serveur d'installation pour toutes les plateformes UNIX.

OB2-TS-CFP	Logiciel commun des composants technologiques du Serveur d'installation pour toutes les plateformes UNIX.
OB2-DAP	Packages d'installation distante de l'agent de disque pour tous les systèmes UNIX.
OB2-MAP	Packages d'installation distante de l'agent de support pour tous les systèmes UNIX.
OB2-NDMPP	Composant de l'agent de support NDMP.
OB2-CCP	Packages d'installation distante de la console de cellule pour tous les systèmes UNIX.

Si d'autres composants Data Protector sont installés sur le système, d'autres composants seront également listés.

Pour une liste complète des composants et des dépendances, voir Dépendances des composants logiciels Data Protector sur Linux , Page 240.

> **REMARQUE :**
> Pour conserver l'installation d'autres composants de Data Protector, vous devez conserver le composant OB2-CORE car il est interdépendant des autres composants.

3. Dans l'ordre inverse de la séquence d'installation, supprimez les composants mentionnés au cours de l'étape précédente en utilisant la commande `rpm -e` *`package name`* et en répondant aux invites.

Suppression manuelle du logiciel Data Protector sur UNIX

Avant de désinstaller un client UNIX, vous devez l'exporter d'une cellule. Pour connaître la procédure, voir Exportation de clients d'une cellule, Page 198.

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 restants à l'aide de la commande `rm` :

   ```
   rm -fr /var/opt/omni
   rm -fr /etc/opt/omni
   rm -fr /opt/omni
   ```

   À ce stade, les références Data Protector ne doivent plus résider sur votre système.

Systèmes Linux

Pour supprimer manuellement les fichiers d'un système Linux, supprimez-les des répertoires suivants puis supprimez les répertoires en utilisant la commande `rm` :

```
rm -fr /var/opt/omni
rm -fr /etc/opt/omni
```

```
rm -fr /opt/omni
```

Systèmes Solaris

Pour supprimer manuellement les fichiers d'un système Solaris, supprimez-les des répertoires suivants puis supprimez les répertoires en utilisant la commande `rm` :

```
rm -fr /var/opt/omni
```

```
rm -fr /etc/opt/omni
```

```
rm -fr /opt/omni
```

Autres systèmes UNIX et systèmes Mac OS X

Supprimez les fichiers du répertoire suivant et supprimez les répertoires en utilisant la commande `rm` :

```
rm -fr /usr/omni
```

Chapitre 7: Mise à niveau de Data Protector

Ce chapitre vous guidera dans les tâches de mise à niveau et de migration Data Protector.

> **REMARQUE :**
> Pendant l'installation, les ports suivants doivent être ouverts pour Inet :
>
> - Installation de Fresh Data Protector - 5565
> - Installation de Data Protector mise à niveau - 5555

Aperçu de la mise à niveau

Avant de mettre à niveau un produit vers la version existante, pensez aux points suivants :

- Pour obtenir des informations sur les plates-formes et les versions prises en charge et arrêtées, consultez les dernières matrices de prise en charge dans https://softwaresupport.softwaregrp.com/ et le Annonces sur les produits, notes sur les logiciels et références Data Protector.

  Sur les plates-formes ne prenant plus en charge Gestionnaire de cellule, commencez par migrer Gestionnaire de cellule vers une plate-forme adéquate, puis mettez à niveau vers Data Protector 10.00. Pour plus d'informations, voir Migrer Gestionnaire de cellule vers une autre plate-forme, Page 258.

  N'étant pas une zone fonctionnelle prise en charge, l'interface utilisateur graphique Java de Data Protector n'est pas fournie dans Data Protector 10.00. Si votre cellule Data Protector compte des systèmes UNIX équipés d'une interface graphique Java Data Protector, vous devrez choisir d'autres systèmes capables de jouer le rôle de clients d'interface graphique Data Protector lors de la mise à niveau. Ces clients doivent fonctionner sur des systèmes d'exploitation pris en charge par l'interface graphique originale (native) Data Protector.
- Les mots de passe de licence délivrés pour les versions antérieures à Data Protector 10.00 ne fonctionneront plus.

  Vous devez disposer d'un accord d'assistance activé pour pouvoir recevoir les nouveaux mots de passe, suivant le type et le nombre de licences indiqués dans votre accord.

  Avant de lancer la mise à niveau, vérifiez le nombre et le type de clés de licence installées dans votre environnement Data Protector et comparez-les à ceux indiqués dans votre accord d'assistance.

  S'ils ne correspondent pas, ne lancez pas la mise à niveau. Il existe sinon un risque que votre environnement Data Protector ne soit plus fonctionnel en raison des clés de licence manquantes. À la place, contactez votre représentant ou votre partenaire pour déterminer les étapes à suivre, afin de mettre à jour les fonctionnalités sous licence du contrat et celles utilisées dans les versions Data Protector antérieures à Data Protector 9.00.

  Pour plus de détails sur les licences, voir Data Protector Licensing, Page 279.
- Une fois la mise à niveau terminée, Gestionnaire de cellule et Serveur d'installation doivent partager la même version Data Protector. Même si les versions antérieures de l'Agent de disque et Agent de support Data Protector sont prises en charge dans la même cellule, il est vivement recommandé d'installer les mêmes composants de Data Protector sur les clients.

Pour plus d'informations sur les contraintes imposées par des versions antérieures d'Agent de disque et de support après une mise à niveau, consultez *Data Protector, Références, notes de publication et annonces produits*.

- Après la mise à niveau d'un environnement à cellules multiples (MoM) tous les Gestionnaire de cellules doivent utiliser la même version de Data Protector.
- Avec Data Protector 10.00, les planificateurs de base et avancé sont obsolètes, et remplacés par un nouveau planificateur Web. Toutes les planifications existantes sont automatiquement migrées vers le nouveau planificateur. La migration ne nécessite aucune interaction de l'utilisateur.

  Si la migration échoue au cours de la mise a niveau, vous pouvez exécuter manuellement la commande suivante pour réussir la migration des planifications existantes vers le nouveau planificateur :

  ```
  omnidbutil -migrate_schedules
  ```
- Avec Data Protector 10.00, JBoss 7.1 est remplacé par WildFly 10. Durant la mise à niveau de Data Protector, les configurations JBoss suivantes sont migrées automatiquement vers WildFly :
  - Niveaux et formats de journalisation
  - Configuration LDAP
  - Données d'identification PostgreSQL

  > **IMPORTANT :**
  > Toutes les modifications apportées au fichier JBoss 7.1 `standalone.xml`, hormis les configurations énumérées ci-dessus, doivent être ajoutées manuellement dans le fichier de configuration de WildFly après la mise à niveau.

  Il est à noter que durant la mise à niveau, Data Protector crée une sauvegarde des anciens fichiers de configuration JBoss dans le dossier Data_Protector_program_data. Par défaut, ces fichiers se trouvent à l'emplacement suivant :
  - Linux : `/etc/opt/omni/server/AppServer_<versionNo>`
  - Windows : `C:\ProgramData\OmniBack\Config\Server\AppServer_<versionNo>`

Conditions préalables

- Lancez des vérifications de base de données sur les IDB existants avant la mise à jour, afin de vous assurer de leur bon fonctionnement.
- Effectuez une sauvegarde du système Gestionnaire de cellule existant et de la base de données interne (IDB).
- Avant de procéder à la mise à niveau, assurez-vous que toutes les requêtes GRE Power On sont fermées. De plus, assurez-vous que les sessions Migration en direct en cours d'exécution sont terminées ou annulées.

Limites

- Il n'est pas possible de changer la plate-forme Gestionnaire de cellule durant la mise à niveau. Les mises à niveau ne sont prises en charge que sur la même plate-forme Gestionnaire de cellule (HP-UX vers HP-UX, Linux vers Linux et Windows vers Windows).

  Si votre plate-forme n'est plus d'actualité, migrez les Gestionnaire de cellule vers une plate-forme compatible et passez à la nouvelle version. Voir Migrer Gestionnaire de cellule vers une autre plate-forme, Page 258.
- Dans un environnement UNIX : Les services Data Protector sont les seuls processus Data Protector capables de fonctionner avant la mise à niveau. Pour ce faire, interrompez les services Data Protector, terminez les processus en cours et relancez les services.
- La restauration de base de données interne n'est prise en charge qu'à partir de la même version Data Protector mineure, dans laquelle la base de données interne a été sauvegardée. Ceci est dû aux changements de schéma de base de données interne présents dans les nouvelles versions.
- Si vous voulez restaurer la base de données interne ayant été sauvegardée dans une version Data Protectorantérieure, réinstallez la version spécifique, importez les supports de sauvegarde de la base de données interne, puis procédez à la restauration.

Séquence de mise à niveau

Pour mettre votre cellule à niveau depuis des versions antérieures du produit, suivez ces étapes :

1. Procédez à une mise à niveau de Gestionnaire de cellule et Serveur d'installation vers Data Protector 10.00. Ces étapes sont différentes sous UNIX et Windows.

   Vous devez d'abord mettre à niveau le Gestionnaire de cellule dans la cellule actuelle avant d'effectuer celle de Serveur d'installation.
2. Mise à niveau des clients GUI.
3. Mettez à niveau les clients équipés d'une intégration d'application en ligne, comme Oracle, SAP R/3, Informix Server, Microsoft SQL Server, Microsoft Exchange Server etc.
4. Mettez à niveau les clients équipés d'un Agent de support Data Protector. Vous pouvez lancer une sauvegarde dès que l'Agent de support est à niveau sur tous les clients de la même plate-forme que Gestionnaire de cellule.
5. Micro Focus recommande une mise à niveau des clients équipés d'un Agent de disque Data Protector dans les deux semaines.

Mise à niveau dans un environnement MoM

Pour faire passer votre environnement MoM vers Data Protector 10.00, vous devez commencer par mettre à niveau le Gestionnaire MoM. Une fois l'opération effectuée, toutes les versions antérieures de Gestionnaire de cellules, qui n'ont pas encore été sauvegardées, peuvent accéder au MMDB et à la licence centrale et effectuer des sauvegardes. Les autres fonctionnalités MoM ne sont pas disponibles. Remarque : le partage d'appareil entre la cellule MoM Data Protector 10.00 et les cellules des versions antérieures du produit n'est pas pris en charge. Au cours de la mise à niveau dans un environnement MoM, aucun des Gestionnaire de cellules de l'environnement MoM ne doit être opérationnel.

Prise en charge pour les anciennes versions des agents

Chaque fois que possible, les composants Data Protector sur tous les clients dans une cellule Data Protector doivent être mis à niveau vers la version 10.00 pendant le processus de mise à niveau normal. Ceci garantit que les clients peuvent bénéficier de toutes les fonctionnalités de Data Protector 10.00 sur tous les systèmes dans une cellule.

Toutefois, les composants Agent de disque et Agent de support d'une version antérieure de Data Protector sont pris en charge dans une cellule 10.00 avec les contraintes suivantes :

- La version antérieure du produit est toujours prise en charge en tant que produit indépendant. Pour connaître les dates de cessation de prise en charge annoncées des produits, consultez la page https://softwaresupport.softwaregrp.com/.
- Le support est limité à l'ensemble de fonctionnalités de la version antérieure de Data Protector.
- Si vous effectuez des opérations impliquant des clients hébergés sur différents systèmes, tous les agents du même type (par exemple les instances Media Agent) doivent être de version identique.
- Les versions antérieures des composants Media Agent ne sont pas prises en charge en combinaison avec les serveurs NDMP.
- Une sauvegarde de système de fichiers peut avoir pour source plusieurs agents de disque avec différentes versions et la déduplication du serveur de sauvegarde est prise en charge avec différentes versions de l'agent de support. Les versions de l'agent de disque et de l'agent de support peuvent être inférieures ou égales à la version du gestionnaire de cellule. Toutefois, la déduplication source nécessite les mêmes versions des agents de disque et des agents de support, qui peuvent être inférieures ou égales à la version du gestionnaire de cellule.
- Pour la banque logicielle Data Protector, l'agent de disque et l'agent de support doivent avoir la même version. Toutefois, cette version peut être inférieure ou égale à la version du gestionnaire de cellule.
- Si un composant Data Protector d'un client est mis à niveau vers la version 10.00, tous les autres éléments doivent également être mis à niveau vers la version 10.00.
- Les versions inférieures des agents d'intégration ne sont pas prises en charge avec la dernière version du gestionnaire de cellule.

Si vous rencontrez des difficultés pour établir une connexion à des agents d'une version de produit antérieure, envisagez d'effectuer une mise à niveau vers la version 9.08 comme première étape de résolution du problème.

Mise à jour de Single Server Edition

Vous pouvez effectuer une mise à niveau depuis :

- Des versions antérieures de la Single Server Edition (SSE) vers Data Protector 10.00 Single Server Edition. Pour plus de détails, consultez Mise à niveau des versions antérieures de SSE vers Data Protector 10.00 SSE.
- De Data Protector 10.00 Single Server Edition vers Data Protector 10.00. Pour plus de détails, consultez Mise à niveau de Data Protector 10.00 SSE vers Data Protector 10.00

Mise à niveau des versions antérieures de SEE vers Data Protector 10.00 SSE

La procédure de mise à niveau des versions antérieures de SEE vers Data Protector 10.00 SSE est la même que pour un passage de Data Protector à Data Protector 10.00.

Mise à niveau de Data Protector 10.00 SSE vers Data Protector 10.00

Il vous faut une licence pour effectuer la mise à niveau de Data Protector 10.00 Single Server Edition vers Data Protector 10.00. Pour plus de détails sur les licences, voir Data Protector Licensing, Page 279.

Deux scénarios sont possibles pour la mise à niveau de Data Protector 10.00 Single Server Edition vers Data Protector 10.00:

- Si vous avez installé Data Protector Single Server Edition sur un seul système (Gestionnaire de cellule). Voir Mise à niveau de Gestionnaire de cellule, bas.
- Si Data Protector Single Server Edition est installé sur plusieurs systèmes et que vous souhaitez fusionner ces cellules. Voir Mise à niveau depuis plusieurs installations, bas.

> **REMARQUE :**
> Pour une mise à niveau depuis une version antérieure de Single Server Edition vers une installation Data Protector complète, commencez par faire passer votre Single Server Edition vers une version complète de même niveau.

Mise à niveau de Gestionnaire de cellule

Pour mettre à niveau Single Server Edition Gestionnaire de cellule, suivez ces étapes :

1. Supprimer la licence Single Server Edition :

   Systèmes Windows :

   ```
   del données_programme_Data_Protector\Config\server\Cell\lic.dat
   ```

   Systèmes UNIX :

   ```
   rm /etc/opt/omni/server/cell/lic.dat
   ```

2. Lancer le GUI Data Protector et ajouter un mot de passe permanent.

Mise à niveau depuis plusieurs installations

Pour mettre à niveau Data Protector Single Server Edition installé sur plusieurs systèmes, suivez ces étapes :

1. Sélectionner l'un des systèmes Single Server Edition existants comme nouveau Gestionnaire de cellule. Voir Choisir le système du Gestionnaire de cellule, Page 23.
2. Mettre à niveau le Gestionnaire de cellule sélectionné en suivant ces étapes :

a. Supprimer la licence Single Server Edition :

   `del` *`données_programme_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. Lancer le GUI Data Protector et ajouter un mot de passe permanent.

3. Importer les autres systèmes Single Server Edition dans le nouveau système Gestionnaire de cellule en tant que clients, par le GUI.
4. Désinstaller le Data Protector Single Server Edition des autres systèmes. Voir .
5. Importer les supports sur le nouveau Gestionnaire de cellule.

   Pour plus d'informations sur l'importation de supports, consultez l'index *Aide de Data Protector* : "importation de supports".

Migrer Gestionnaire de cellule vers une autre plate-forme

Migration des systèmes PA-RISC HP-UX vers Intel Itanium HP-UX

Data Protector ne prend plus en charge l'architecture PA-RISC basée sur HP-UX 11.11/11.23 comme plate-forme Gestionnaire de cellule. Vous devez donc migrer Gestionnaire de cellule depuis une architecture PA-RISC basée sur un système HP-UX 11.11/11.23 vers un HP-UX 11.23/11.31 pour architecture Intel Itanium 2 avant la mise à niveau.

Pour un résumé de la procédure, consultez le *Guide d'installation Data Protector* du produit adéquat.

Migration de Windows 32-bit/64-bit à Windows64-bit/Windows Server 2008 ou Windows Server 2012

Data Protector ne prend plus en charge les systèmes Windows 32-bit comme plates-formes Gestionnaire de cellule. Vous devez donc migrer le Gestionnaire de cellule vers un système Windows 64-bit avant de lancer la procédure de mise à niveau vers Data Protector 10.00 ou des versions ultérieures. Pour un résumé de la procédure, consultez le *Guide d'installation Data Protector* du produit adéquat.

Migration de Solaris à Linux

Cette section décrit la procédure de migration de votre Gestionnaire de cellule d'un système Solaris à un système Linux.

> **IMPORTANT :**
> Data Protector 10.00 ne prend plus en charge Solaris comme plate-forme Gestionnaire de cellule. Vous devez donc migrer la Gestionnaire de cellule vers une nouvelle plate-forme avant

de lancer la procédure de mise à niveau vers Data Protector 10.00 ou des versions ultérieures, à l'aide de la version installée de Data Protector.

Procédure

1. Via votre installation existante de Data Protector, exportez tous les catalogues de supports sur le Gestionnaire de cellule courant :
   a. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
   b. Dans la fenêtre de navigation, développez **Supports**, puis **Pools**.
   c. Développez le pool contenant le support dont vous souhaitez copier le catalogue.
   d. Cliquez avec le bouton droit sur le support, puis choisissez **Copier le catalogue** dans un fichier.
   e. Indiquez le répertoire de sortie pour les fichiers MCF, qui contiendront les données de catalogue relatives aux supports.
   f. Cliquez sur **Terminer** pour lancer la copie et quitter l'assistant. Pour plus de détails, consultez le sujet *Aide de Data Protector Copie des données des supports du catalogue dans le fichier MCF*.
2. Installez Data Protector sur le système Linux qui deviendra le nouveau Gestionnaire de cellule. Pour plus d'informations, voir Installing a UNIX Gestionnaire de cellule, Page 27.
3. Si vous avez changé le port Inet Data Protector par défaut sur l'ancien Gestionnaire de cellule, paramétrez le même sur le nouveau Gestionnaire de cellule. Voir Changer le port Inet par défaut Data Protector, Page 354.
4. Importez les fichiers MCF sur le nouveau Gestionnaire de cellule :
   a. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
   b. Dans la fenêtre de navigation, développez **Supports**, cliquez avec le bouton droit de la souris sur **Pools**, puis cliquez sur **Importer le catalogue à partir du fichier MCF** pour lancer l'assistant.
   c. Spécifiez les fichiers MCF que vous souhaitez importer.
   d. Spécifiez des options supplémentaires pour la session : par défaut, l'option **Importer dans le pool d'origine si possible** est sélectionnée. Sélectionner **Importer la copie comme étant l'original**.
   e. Cliquez sur **Terminer** pour démarrer l'importation et quitter l'assistant.

   Pour plus de détails, consultez le sujet *Aide de Data Protector Importer les données des supports du catalogue depuis le fichier MCF*.
5. Configurer les licences sur le nouveau Gestionnaire de cellule. Voir Data Protector Structure et licences de produit, Page 308.
6. D'autres étapes sont requises dans le cas suivant :
   - Votre cellule appartient à l'environnement MoM. Voir Spécificités MoM, Page suivante.
   - Votre cellule fonctionne derrière un pare-feu. Reconfigurez tous les paramètres associés du pare-feu sur le nouveau Gestionnaire de cellule. Reportez-vous à l'index *Aide de Data Protector* : "environnements pare-feu".

- Vous souhaitez avoir un Serveur d'installation sur votre nouveau Gestionnaire de cellule. Voir Serveur d'installation spécificités, bas.

Une fois la migration terminée, vous pouvez mettre à niveau Data Protector.

Spécificités MoM

Si le nouveau Gestionnaire de cellule doit être configuré dans le MoM, d'autres étapes sont nécessaires après la migration de base. Les étapes requises dépendent de la configuration du MoM de vos anciens et nouveaux Gestionnaire de cellule dans votre environnement. Combinaisons prises en charge :

- 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. Sur le Gestionnaire MoM, exportez l'ancien Gestionnaire de cellule de la cellule du Gestionnaire MoM et importez le nouveau Gestionnaire de cellule. Reportez-vous à l'index *Aide de Data Protector* : "systèmes clients:exportation".
  2. Ajoutez l'administrateur MoM sur la liste des utilisateurs du nouveau Gestionnaire de cellule. Reportez-vous à l'index *Aide de Data Protector* : "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 n'était qu'un client du MoM, aucune action n'est requise. Dans le cas contraire, suivez ces étapes :

  1. Sur l'ancien Gestionnaire MoM (ancien Gestionnaire de cellule), exportez tous les clients MoM.
  2. Sur le nouveau Gestionnaire MoM (nouveau Gestionnaire de cellule), importez tous les clients MoM.
  3. Ajoutez l'administrateur MoM sur la liste des utilisateurs sur tous les clients MoM.

Serveur d'installation spécificités

La migration du Serveur d'installation n'entre pas dans la migration du Gestionnaire de cellule. Si 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.

Pour utiliser le nouveau Gestionnaire de cellule comme Serveur d'installation, installez le composant Serveur d'installation sur le nouveau Gestionnaire de cellule après la migration et l'importation dans la cellule. Reportez-vous à l'index *Aide de Data Protector* : "Serveur d'installation".

Migrer une base de données interne Gestionnaire de cellule Windows vers un autre serveur

Le scénario qui suit est un exemple de migration d'IDB d'un serveur Gestionnaire de cellules Windows vers un autre.

Terminologie

Nous utilisons la terminologie suivante dans ce scénario.

- **OLD_SERVER**. Le Gestionnaire de cellule source depuis lequel l'IDB sera déplacé.
- **NEW_SERVER.** Le Gestionnaire de cellule de destination vers lequel l'IDB sera déplacé.

Conditions préalables

- Lorsque vous utilisez des arguments de commande, substituez tout le nom de domaine : OLD_SERVER et NEW_SERVER.
- Si OLD-SERVER fonctionne sous Windows 2008, NEW-SERVER peut fonctionner sous Windows 2008 ou Windows 2012.
- Si OLD-SERVER fonctionne sous Windows 2012, NEW-SERVER doit fonctionner sous Windows 2012.
- Les deux serveurs doivent être équipés d'une version identique de Data Protector sur le Gestionnaire de cellule.
- Si NEW_SERVER n'a pas la même adresse IP que OLD_SERVER, vous devez déplacer vos licences vers la nouvelle adresse IP en contactant le Centre de remise de mots de passe (https://software.microfocus.com/fr-fr/legal/software-licensing).
- Sur NEW_SERVER, vous devez pouvoir importer les supports qui contiennent la sauvegarde complète de l'IDB depuis OLD-SERVER.
  - Si la sauvegarde de l'IDB se trouve sur une bande physique, vous devez configurer un lecteur ou une bibliothèque sur NEW-SERVER et vous assurer que la bande est bien accessible.
  - Si la sauvegarde de l'IDB se trouve sur un périphérique de bibliothèque de fichiers, vous devrez peut-être exporter celle-ci depuis OLD_SERVER et l'importer vers NEW_SERVER. Pour plus d'informations, reportez-vous à NEW_SERVER, Page suivante.
- La configuration, les journaux et les fichiers de bases de données sont stockés sous le répertoire *données_programme_Data_Protector*, généralement `C:\ProgramData\Omniback`.

  Si vous faites une installation ailleurs, notez son emplacement pour une utilisation ultérieure.

Préparer la migration

Avant de commencer la migration, plusieurs tâches doivent être accomplies sur OLD_SERVER et NEW_SERVER afin de les préparer pour la migration de l'IDB.

OLD_SERVER

- Lancez des vérifications de base de données avancées sur les IDB existants sur OLD_SERVER, afin de vous assurer de leur cohérence.
- Lancez une sauvegarde complète de l'IDB existant.

Lancer une vérification de base de données avancée

1. Exécutez `omnidbcheck -extended`.

   Cette commande valide la cohérence des données dans les zones suivantes :

   - Connexion base de données
   - Cohérence de la base de données et du schéma
   - Cohérence des fichiers et des supports

   En cas d'incohérence, réglez le problème avant d'effectuer la migration.

Effectuer une sauvegarde complète de l'IDB sur OLD_SERVER

Pour plus d'informations sur la sauvegarde complète de l'IDB, voir *Aide de Data Protector*.

NEW_SERVER

- Sauvegardez une copie du fichier `cell_info` , placé dans le répertoire *données_programme_Data_Protector*, généralement `C:\ProgramData\Omniback\Config\Server\cell\cell_info`. Ce fichier servira plus tard.

Utiliser omnidownload et omniupload pour transférer les infirmations sur la bibliothèque de fichiers

1. Sur OLD_SERVER, utilisez `omnidownload-library` *`Library`* pour télécharger des informations sur la bibliothèque de fichiers depuis l'IDB Data Protector vers un fichier ASCII.

   Exemple : pour une sauvegarde IDB vers une bibliothèque de fichiers nommée "FL1", utilisez la commande comme suit :

   ```
   omnidownload –library FL1 –file “C:\tmp\FL1.txt”
   ```

2. Copiez le fichier de sortie `omnidownload` sur NEW_SERVER.

   Par exemple, copiez vers `C:\tmp\FL1.txt`.

3. Sur NEW_SERVER, utilisez omniupload -create_library <filename>.txt pour charger le fichier bibliothèque et créez un nouveau périphérique de sauvegarde sur NEW_SERVER.

   ```
   omniupload -create_library “C:\tmp\FL1.txt”
   ```

4. Importez les supports du nouveau périphérique de sauvegarde sur NEW_SERVER.

   Pour plus de détails sur les commandes, voir *Guide de référence de l'interface de ligne de commande Data Protector*. Pour plus de détails sur l'importation de supports, voir *Aide de Data Protector*.

Tâches de migration

Conditions préalables sous Linux :

- Si l'IDB est restauré vers un nouvel hôte ou gestionnaire de cellule, `user` et `group ID` doivent être identiques à ceux du gestionnaire de cellule d'origine.

Utilisez les commandes suivantes pour modifier `user` et `group ID` sur le nouvel hôte avant d'installer Data Protector :

- Pour déterminer l'ID de `hpdp user` et `group` sur l'hôte d'origine, utilisez `cat /etc/passwd`.
- Pour configurer `user` et `group ID` sur le nouvel hôte, utilisez :

  ```
  usermod -u <NEWID> <LOGIN>
  groupmod -g <NEWID> <GROUP>
  usermod -g <GROUP> <LOGIN>
  ```

Importer l'IDB

Pour importer l'IDB sur NEW_SERVER

1. Une fois les supports importés, assurez-vous de bien voir la session de sauvegarde IDB sur le GUI Data Protector.
2. Créez un nouveau répertoire pour la restauration IDB.

   Créez par exemple un répertoire à l'emplacement suivant :

   ```
   C:\ProgramData\Omniback\server\db80_restore\idb
   ```

   > **REMARQUE :** Vous ne pouvez pas restaurer l'IDB de OLD_SERVER au même emplacement sur NEW_SERVER, car celui-ci est utilisé.

3. Dans la liste de contexte Data Protector, cliquez sur **Restaurer**.
4. Dans la fenêtre de navigation, développez **Restaurer des objets**, puis **Base de données interne**.
5. Développez OLD_SERVER et cliquez sur **Base de données interne**.
   a. Sur la page de propriétés, pour restaurer les composants de base de l'IDB :
      i. Sélectionnez **Restaurer la base de données interne**.
      ii. Spécifiez le port temporaire de l'IDS pendant la restauration, ainsi que son emplacement : `C:\ProgramData\Omniback\server\db80_restore\idb`.
      iii. Sélectionnez **Restaurer les fichiers binaires** du catalogue pour restaurer le DCBF de l'IDB, puis **Restaurer vers emplacement d'origine**.
   b. Sur la page de propriétés des Fichiers de configuration :

      Sur un système Windows :

      i. Sélectionnez **Restaurer vers emplacement d'origine**.

      > **REMARQUE :**
      > Assurez-vous que l'option **Restaurer les fichiers de configuration** est bien cochée.

      ii. Sélectionnez Garder le plus récent dans la liste **Gestion de conflit de fichiers**.

      Sur un système UNIX :

      Voir Échec de la restauration de l'IDB à la fin d'un processus de restauration, Page 268
   c. Cliquez sur **Restaurer** pour démarrer le processus de restauration de l'IDB.

Au cours de la restauration, il est possible que le message d'erreur suivant s'affiche, ainsi que d'autres, qui peuvent être ignorés :

```
[Major] From: OB2BAR_POSTGRES_BAR@mrou77.usa.hp.com "DPIDB" Time: 10/9/2014
10:35:29 PM The OS reported error while accessing
C:/ProgramData/OmniBack/config/server/certificates: [80] The file exists.
```

d. Une fois l'opération terminée, interrompez et relancez les services Data Protector.

```
omnisrv -stop
```

```
omnisrv -start
```

> **REMARQUE :**
> Si vous avez le moindre problème une fois la session de restauration de l'IDB terminée, consultez le Dépannage.

Tâches après restauration

Effectuez ces tâches après restauration.

1. Exécutez `omnidbutil -show_db_files` pour vous assurer que les fichiers restaurés sont bien dans le répertoire créé à l'étape 3 de Importer l'IDB, Page précédente.
2. Ajoutez NEW_SERVER comme Gestionnaire de cellule. Voir Ajouter NEW_SERVER comme Gestionnaire de cellule, bas
3. Vous pouvez aussi changer le nom de Gestionnaire de cellule dans l'IDB. Voir Changer le nom Gestionnaire de cellule dans l'IDB, Page suivante.
4. Exécutez `omnidbcheck -extended` pour vérifier la cohérence de l'IDB restauré. Voir Lancer une vérification de base de données avancée , Page 262.

Ajouter NEW_SERVER comme Gestionnaire de cellule

Pour ajouter NEW_SERVER comme Gestionnaire de cellule.

1. Dans la liste de contexte Data Protector, cliquez sur **Clients**.
2. Supprimez l'ancien objet OLD_SERVER.
3. Importez NEW_SERVER et assurez-vous qu'il apparaît comme Gestionnaire de cellule.

Si l'opération ne fonctionne pas

1. Dans un éditeur de texte, ouvrez le fichier `cell_info` sauvegardé dans Préparer la migration, Page 261.
2. Copiez la ligne contenant le nom d'hôte de NEW_SERVER dans votre tampon de collage.
3. Modifiez le fichier `cell_info`.
   a. Ajoutez l'entrée de NEW_SERVER depuis le tampon.
   b. Supprimez l'entrée OLD_SERVER et sauvegardez le fichier `cell_info`.
4. Relancez l'interface utilisateur.

Changer le nom Gestionnaire de cellule dans l'IDB

Si NEW_SERVER a un nom d'hôte différent de OLD_SERVER, vous devez changer le nom Gestionnaire de cellule dans l'IDB.

Par exemple, OLD_SERVER se nomme `oldcm.company.com` et NEW_SERVER se nomme `newcm.company.com`.

Sur NEW_SERVER

1. Exécutez `omnidbutil -show_cell_name` pour afficher le Gestionnaire de cellule de l'IDB.

   Par exemple :

   ```
   > omnidbutil -show_cell_name
   Propriétaire base de données catalogue : "oldcm.company.com"
   ```

2. Exécutez `-change_cell_name` *`OldHost`* pour changer le propriétaire de l'IDB dans NEW_SERVER.

   Par exemple :

   ```
   > omnidbutil -change_cell_name oldcm.company.com
   This action will change ownership of libraries, devices, media pools and media.
   Are you sure [y/n]? y
   DONE!
   ```

Étapes suivantes

1. Migrez vos clients vers NEW_SERVER en exécutant la commande `omnicc` .

   Exécutez la commande `omnicc -update_all -force_cs` pour mettre à jour la version et les informations des composants installés dans le fichier de configuration cell_info NEW_SERVER pour tous les clients de la cellule.

   Pour une description des commandes `omnicc`, voir *Guide de référence de l'interface de ligne de commande Data Protector*.

2. Créez une nouvelle spécification de sauvegarde IDB pour NEW_SERVER, car l'original est configuré pour utiliser OLD_SERVER.

   Pour plus d'informations, reportez-vous à la section *Aide de Data Protector*.

3. Naviguez vers l'IDB et vérifiez si des sessions sont en cours d'exécution. Si des sessions sont en cours, exécutez la commande `omnidbutil -clear`.

4. Arrêtez et lancez les services Data Protector.

   omnisrv -stop

   omnisrv -start

Dépannage

Problème

Une fois l'opération de restauration de l'IDB terminée, la connexion depuis le GUI Data Protector vers Gestionnaire de cellule échoue.

Une fois l'opération de restauration terminée, la connexion depuis le GUI vers Gestionnaire de cellule échoue, avec l'erreur :

```
Une erreur de serveur s'est produite. Message d'erreur rapporté :
couldn't connect to host.
```

Le processus de service `hpdp-as` n'apparaît pas sur le port 7116.

Action

1. Vérifiez le port d'écoute 7116 en ouvrant la fenêtre de commande et en exécutant la commande netstat.

   ```
   c:\> netstat -ban | findstr 7116 | findstr LISTEN
   ```

   Si la commande netstat renvoie des résultats, le port d'écoute est correctement configuré.

   Dans le cas contraire, la configuration a échoué, exemple :

   ```
   c:\> netstat -ban | findstr 7116 | findstr LISTEN
   c:\>
   ```

2. Enregistrez une sauvegarde du fichier `/etc/opt/omni/server/AppServer/standalone.xml`.
3. Remplacez toutes les banques de clés et banques d'approbations dans par celles stockées dans `/etc/opt/omni/server/AppServer/standalone.xml` par celles stockées dans `/etc/opt/omni/client/components/webservice.properties`.

   Naviguez vers le répertoire `C:\ProgramData\Omniback\Config\client\components` et dans le fichier `webservice.properties`, puis recherchez les lignes de code suivantes :

   ```
   keystorePassword=jones7XE7EJjHzZ
   ```

   ```
   truststorePassword=jones7XE7EJjHzZ
   ```

4. Notez le mot de passe de la banque de clés pour plus tard.
5. Ouvrez le fichier `standalone.xml` dans un éditeur de texte et recherchez les lignes qui contiennent `keystore-password`, comme :

   ```
   <jsse keystore-password="JypjEncO.9aG1"
   keystoreurl="C:/ProgramData/OmniBack/Config/server/certificates/server/server.k
   eystore"
   ```

   ```
   truststore-password="JypjEncO.9aG1"
   truststoreurl="C:/ProgramData/OmniBack/Config/server/certificates/server/server
   .truststore"/>
   ```

6. Remplacez les mots de passe `keystore` et `truststore` dans le fichier `standalone.xml` par le mot de passe de banque de clés du fichier `webservice.properties` de l'étape 4 et ernegistrez le fichier.

7. Dans une fenêtre de commande, accédez à `C:\Program Files\OmniBack\bin`.
8. Regénérez le certificat avec la commande suivante :

   ```
   perl omnigencert.pl -server_id NEW_SERVER -store_password <keystore-password>
   ```

   où ***<keystore-password>*** est le mot de passe noté à l'étape 4.
9. Arrêtez et lancez les services Data Protector.

   ```
   omnisrv -stop
   ```

   ```
   omnisrv -start
   ```
10. Essayez de vous connecter au Gestionnaire de cellule.

Problème

Une fois l'opération de restauration de l'IDB terminée, la connexion depuis le GUI Data Protector vers Gestionnaire de cellule échoue avec des erreurs SSL

Une fois l'opération de restauration terminée, la connexion depuis le GUI vers Gestionnaire de cellule échoue, avec l'erreur :

```
Une erreur de serveur s'est produite. Message d'erreur rapporté :
SSL peer certificate or SSH remote was not OK.
```

Action

1. Accédez au répertoire `C:\ProgramData\Omniback\Config\client\components` et ouvrez le fichier `webservice.properties` :

   ```
   # global property file for all components
   jce-serviceregistry.URL = https://newcm.company.com:7116/jce-
   serviceregistry/restws

   keystorePath=C:/ProgramData/OmniBack/Config/server/certificates/client/client.k
   eystore

   truststorePath=C:/ProgramData/OmniBack/Config/server/certificates/client/client
   .truststore
   keystorePassword=jones7XE7EJjHzZ
   truststorePassword=jones7XE7EJjHzZ
   ```
2. Notez le `keystorePassword` et le `truststorePassword`.
3. Dans une fenêtre de commande, accédez à `C:\Program Files\OmniBack\bin`.
4. Regénérez le certificat avec la commande suivante :

   ```
   perl omnigencert.pl -server_id NEW_SERVER -store_password <keystore-password>
   ```

   où ***<keystore-password>*** est le mot de passe noté à l'étape 2.
5. Arrêtez et lancez les services Data Protector.

   ```
   omnisrv -stop
   ```

   ```
   omnisrv -start
   ```
6. Essayez de vous connecter au Gestionnaire de cellule.

Problème

Pendant une sauvegarde d'IDB, l'IDB ne peut être mis en mode sauvegarde et se met en échec

Pendant une sauvegarde IDB, les Messages de sessions indiquent une erreur :

```
[Critique] De : OB2BAR_POSTGRES_BAR@oldcm.company.com "DPIDB" Time: 10/10/2014
12:19:51 PM

Putting the Internal Database into the backup mode failed
```

Action

1. Accédez à `C:\ProgramData\OmniBack\Config\Server\idb` and made et faites une copie de sauvegarde du fichier `idb.config`.
2. Dans un éditeur de texte, ouvrez le fichier idb.config et cherchez `PGOSUSER`.

   Par exemple :

   ```
   PGOSUSER='OLD_SERVER\Administrator';
   ```
3. Si le nom de serveur n'est pas le bon, modifiez-le en NEW_SERVER.

   Par exemple :

   ```
   PGOSUSER='NEW_SERVER\Administrator';
   ```
4. Arrêtez et lancez les services Data Protector.

   ```
   omnisrv -stop

   omnisrv -start
   ```
5. Retentez la sauvegarde de l'IDB.

Problème

Échec de la restauration de l'IDB à la fin d'un processus de restauration

La restauration de l'IDB a échoué à la fin du processus de restauration, en renvoyant le message suivant :

```
Impossible d'exécuter la commande omnidbutil -clear
```

Action

Ceci peut se produire dans un Gestionnaire de cellule HP-UX dans les circonstances suivantes : Lors d'un processus de restauration dans un autre Gestionnaire de cellule ou dans le même Gestionnaire de cellule, mais si les mots de passe postgres ont été modifiés après la restauration de la session de sauvegarde ou après l'installation d'un nouveau Gestionnaire de cellule.

> **REMARQUE :**
> Dans un environnement Linux, la restauration s'effectuera correctement. Ceci s'explique par le fait que Linux utilise généralement l'authentification du système d'exploitation sur d'autres bases de données que HP-UX, qui utilisent l'autorisation par mot de passe et, dans ce cas, les mots de passe ne sont pas restaurés correctement. Cependant, pour disposer des fichiers de mots de passe appropriés, la solution doit également être appliquée aux environnements Linux.

1. Restaurez uniquement les fichiers de configuration vers un autre emplacement `<restore-conf>` jusqu'au point de restauration complète de l'IDB.
2. Procédez à la restauration complète de l'IDB mais ne choisissez pas de restaurer les fichiers binaires de catalogue des détails (DCBF) dans leur emplacement initial.
3. Enregistrement d'une sauvegarde de `/etc/otp/omni/server/idb/idb.config` vers `idb.config.bkp`
4. Effectuez des copies de fichiers de l'emplacement `<restore-conf>` vers l'emplacement d'origine :
   a. `cp <restore-conf>/etc/opt/omni/server/idb/idb.config /etc/opt/omni/server/idb/idb.config`
   b. `cp <restore-conf>/etc/opt/omni/server/idb/ulist /etc/opt/omni/server/idb/ulist`
   c. `cp <restore-conf>/etc/opt/omni/server/AppServer/standalone.xml /etc/opt/omni/server/AppServer/standalone.xml`
5. Modifiez les champs suivants dans le fichier `idb.config` pour pointer vers l'emplacement correct (les emplacements corrects sont stockés dans le fichier `idb.config.bkp`)
   a. `PGDATA_PG='/space/restore1/pg';`
   b. `PGDATA_IDB='/space/restore1/idb';`
   c. `PGDATA_JCE='/space/restore1/jce';`
   d. `PGWALPATH='/space/restore1/pg/pg_xlog_archive' ;`
6. Arrêtez et lancez les services Data Protector.
   a. exécutez la commande `omnisv stop` (ceci peut prendre un certain temps)
   b. exécutez la commande `omnisv start`
   c. exécutez la commande `omnidbutil -clear`

Mise à niveau du Gestionnaire de cellule configuré dans Serviceguard

Lors d'une procédure de mise à niveau, seule la base de données est affectée, la version précédente du produit est supprimée. La dernière versionData Protector est installé avec la sélection d'agents par défaut et les autres sont supprimés. Pour obtenir une configuration équivalente à celle antérieure à la mise à niveau, vous devez sélectionner manuellement les autres agents pendant la procédure ou les réinstaller après, sur chaque nœud physique.

Conditions préalables

- Les services de Data Protector sur le(s) nœud(s) secondaire(s) de Serviceguardne doivent pas fonctionner.

  La mise à niveau peut ainsi utiliser l'IDB exporté pendant la mise à niveau du nœud primaire et évite une exportation supplémentaire.

La procédure de mise à niveau des versions précédentes de Data Protector à la dernière version deData Protector comprend la mise à niveau des nœuds primaires et secondaires. Suivez les instructions dans l'ordre présenté dans les sections ci-dessous.

Nœud primaire

Connectez-vous au nœud primaire et suivez cette procédure :

1. Interrompez l'ancien package Data Protector en lançant la commande `cmhaltpkg *PackageName*`, où *`PackageName`* est le nom du package de cluster). Par exemple :

   ```
   cmhaltpkg ob2cl
   ```
2. Activer le groupe de volumes en mode exclusif :

   ```
   vgchange -a e -q y VGName
   ```

   Par exemple :

   ```
   vgchange -a e -q y /dev/vg_ob2cm
   ```
3. Monter le volume logique sur le disque partagé :

   ```
   mount LVPathSharedDisk
   ```

   Le paramètre *`LVPath`* est le nom de chemin du volume logique et *`SharedDisk`* est le point de montage du répertoire partagé. Par exemple :

   ```
   mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
   ```
4. Démarrez les services Data Protector:

   ```
   omnisv -start
   ```
5. Mettez à niveau Gestionnaire de cellule en suivant les instructions de la section . Certaines étapes diffèrent suivant la version du produit que vous mettez à niveau.
6. Arrêter les services Data Protector :

   ```
   omnisv -stop
   ```
7. Démonter le disque partagé :

   ```
   umount SharedDisk
   ```

   Par exemple :

   ```
   umount /omni_shared
   ```
8. Désactiver le groupe de volumes :

   ```
   vgchange -a n VGName
   ```

   Par exemple :

   ```
   vgchange -a n /dev/vg_ob2cm
   ```

Nœud secondaire

Connectez-vous au nœud secondaire et suivez cette procédure :

1. Activer le groupe de volumes en mode exclusif :

   ```
   vgchange -a e -q y VGName
   ```
2. Monter le volume logique sur le disque partagé :

```
mount LVPathSharedDisk
```

3. Mettez à niveau Gestionnaire de cellule en suivant les instructions de la section . Certaines étapes diffèrent suivant la version du produit que vous mettez à niveau.
4. Renommez les scripts de démarrage `csfailover.sh` et `mafailover.ksh` dans le répertoire `/etc/opt/omni/server/sg` (par exemple vers `csfailover_DP70.sh` et `mafailover_DP70.ksh`) et copiez le nouveau `csfailover.sh` et les scripts `mafailover.ksh` du répertoire `/opt/omni/newconfig/etc/opt/omni/server/sg` vers le répertoire `/etc/opt/omni/server/sg`.

   Si vous avez personnalisé les scripts de démarrage, appliquez de nouveau ces changements.
5. Arrêter les services Data Protector :

   ```
   omnisv -stop
   ```
6. Démonter le disque partagé :

   ```
   umount SharedDisk
   ```
7. Désactiver le groupe de volumes :

   ```
   vgchange -a n VGName
   ```

Nœud primaire

Connectez-vous au nœud primaire et suivez cette procédure :

1. Démarrer le package Data Protector :

   ```
   cmrunpkg PackageName
   ```
2. Configurer le Gestionnaire de cellule. Veillez à ne pas vous placer dans les répertoires `/etc/opt/omni` ou `/var/opt/omni` ni dans leurs sous-répertoires lorsque vous exécutez ce script. Assurez-vous également de ne pas avoir monté de sous-répertoire dans `/etc/opt/omni` ou `/var/opt/omni`. Exécutez :

   ```
   /opt/omni/sbin/install/omniforsg.ksh -primary -upgrade
   ```
3. Arrêtez le package Data Protector :

   ```
   cmhaltpkg PackageName
   ```

Nœud secondaire

Connectez-vous au nœud secondaire et suivez cette procédure :

1. Démarrer le package Data Protector :

   ```
   cmrunpkg PackageName
   ```
2. Configurer le Gestionnaire de cellule. Veillez à ne pas vous placer dans les répertoires `/etc/opt/omni` ou `/var/opt/omni` ni dans leurs sous-répertoires lorsque vous exécutez ce script. Assurez-vous qu'aucun sous-répertoire n'est soit installé dans le répertoire `/etc/opt/omni` ou `/var/opt/omni`. Exécutez :

   ```
   /opt/omni/sbin/install/omniforsg.ksh -secondary /share -upgrade
   ```

   > **REMARQUE :**
   > `/share` est le répertoire ou stockage partagé entre les nœuds de cluster.

3. Arrêtez le package Data Protector :

   ```
   cmhaltpkg PackageName
   ```

Nœud primaire

Connectez-vous à nouveau au nœud primaire et suivez cette procédure :

1. Démarrer le package Data Protector :

   ```
   cmrunpkg PackageName
   ```

   Assurez-vous que les options de changement de packages et de nœuds sont activées.
2. Importer à nouveau l'hôte virtuel :

   ```
   omnicc -import_host VirtualHostname -virtual
   ```
3. Changer le nom Gestionnaire de cellule dans l'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 Serveur d'installation :

   ```
   omnicc -import_is VirtualHostname
   ```

> **REMARQUE :**
> Toutes les requêtes de Gestionnaire de cellule sont enregistrées dans le fichier `/var/opt/omni/log/inet.log` sur les clients Data Protector. Pour éviter les entrées inutiles, sécurisez les clients. Voir À propos de la sécurité, Page 200 pour savoir comment sécuriser une cellule.

Mise à niveau du Gestionnaire de cellule configuré pour Symantec Veritas Cluster Server

Lors d'une procédure de mise à niveau, seule la base de données est affectée, la version précédente du produit est supprimée. Data Protector est installé avec la sélection d'agents par défaut. Les autres sont supprimés. Pour obtenir une configuration équivalente à celle antérieure à la mise à niveau, vous devez sélectionner manuellement les autres agents pendant la procédure ou les réinstaller après, sur chaque nœud physique.

Conditions préalables

Les services de Data Protector sur le(s) nœud(s) secondaire(s) de Symantec Veritas Cluster Server ne doivent pas fonctionner.

La procédure de mise à niveau des versions précédentes de Data Protector comprend la mise à niveau des nœuds primaires et secondaires. Suivez les instructions dans l'ordre présenté dans les sections ci-dessous.

Nœud primaire

Connectez-vous au nœud principal et procédez aux étapes suivantes :

1. Mettez la ressource d'application Data Protector hors ligne.
2. Désactiver la ressource d'application Data Protector.
3. Redémarrez les services Data Protector :

   ```
   omnisv -start
   ```
4. Mettez à niveau Gestionnaire de cellule en suivant les instructions de la section .
5. Si vous avez personnalisé le script de contrôle utilisé par la ressource d'application de Data Protector, remettez en place les modifications fournies par le script `/opt/omni/sbin/vcsfailover.ksh` récemment installé dans votre script personnalisé.
6. Arrêter les services Data Protector :

   ```
   omnisv -stop
   ```

Nœud secondaire

Connectez-vous au nœud secondaire et procédez aux étapes suivantes :

1. Faites basculer le groupe de services Data Protector sur le nœud secondaire.
2. Mettez à niveau Gestionnaire de cellule en suivant les instructions de la section .
3. Si vous avez personnalisé le script de contrôle utilisé par la ressource d'application de Data Protector, remettez en place les modifications fournies par le script `/opt/omni/sbin/vcsfailover.ksh` récemment installé dans votre script personnalisé.
4. Arrêter les services Data Protector :

   ```
   omnisv -stop
   ```

Nœud primaire

Connectez-vous à nouveau au nœud principal et procédez aux étapes suivantes :

1. Faites basculer le groupe de services Data Protector sur le nœud principal.
2. Activer la ressource d'application Data Protector.
3. Mettez la ressource d'application Data Protector en ligne.
4. Configurer le Gestionnaire de cellule. Assurez-vous que le script n’est pas exécuté depuis les répertoires `/etc/opt/omni` ou `/var/opt/omni`, ni l'un de leurs sous-répertoires. Assurez-vous également qu'aucun sous-répertoire n'est monté dans le répertoire `/etc/opt/omni` ou `/var/opt/omni`. Exécuter la commande suivante :

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

Nœud secondaire

Connectez-vous à nouveau au nœud secondaire et procédez aux étapes suivantes :

1. Faites basculer le groupe de services Data Protector sur le nœud secondaire.
2. Configurer le Gestionnaire de cellule. Assurez-vous que le script n'est pas exécuté depuis les répertoires `/etc/opt/omni` ou `/var/opt/omni`, ni l'un de leurs sous-répertoires. Assurez-vous également qu'aucun sous-répertoire n'est monté dans le répertoire `/etc/opt/omni` ou `/var/opt/omni`. Exécuter la commande suivante :

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

   où *dirname* est le point de montage ou répertoire partagé (par exemple `/omni_shared`).

Nœud primaire

Connectez-vous à nouveau au nœud principal et procédez aux étapes suivantes :

1. Faites basculer le groupe de services Data Protector sur le nœud principal.
2. Si le Serveur d'installation se trouve dans le même package que le Gestionnaire de cellule, importez le nom d'hôte virtuel Serveur d'installation :

   ```
   omnicc -import_is VirtualHostname
   ```

> **REMARQUE :**
> Toutes les requêtes de Gestionnaire de cellule sont enregistrées dans le fichier `/var/opt/omni/log/inet.log` sur les clients Data Protector. Pour éviter les entrées inutiles, sécurisez les clients. Voir À propos de la sécurité, Page 200 pour savoir comment sécuriser une cellule.

Mise à niveau du Gestionnaire de cellule configuré sur Microsoft Cluster Server

La mise à niveau du Gestionnaire de cellule sur Microsoft Cluster Server (MSCS) se fait localement, depuis le package d'installation Windows.

Conditions préalables

- L'option de mise à niveau n'est prise en charge que si le logiciel Data Protector installé est le Gestionnaire de cellule installé en mode cluster. Si un système du cluster est équipé du logiciel Data Protector dans un autre mode, vous devez le désinstaller avant de lancer le paramétrage.

Procédure de mise à niveau

Pour effectuer la mise à niveau, suivez ces étapes :

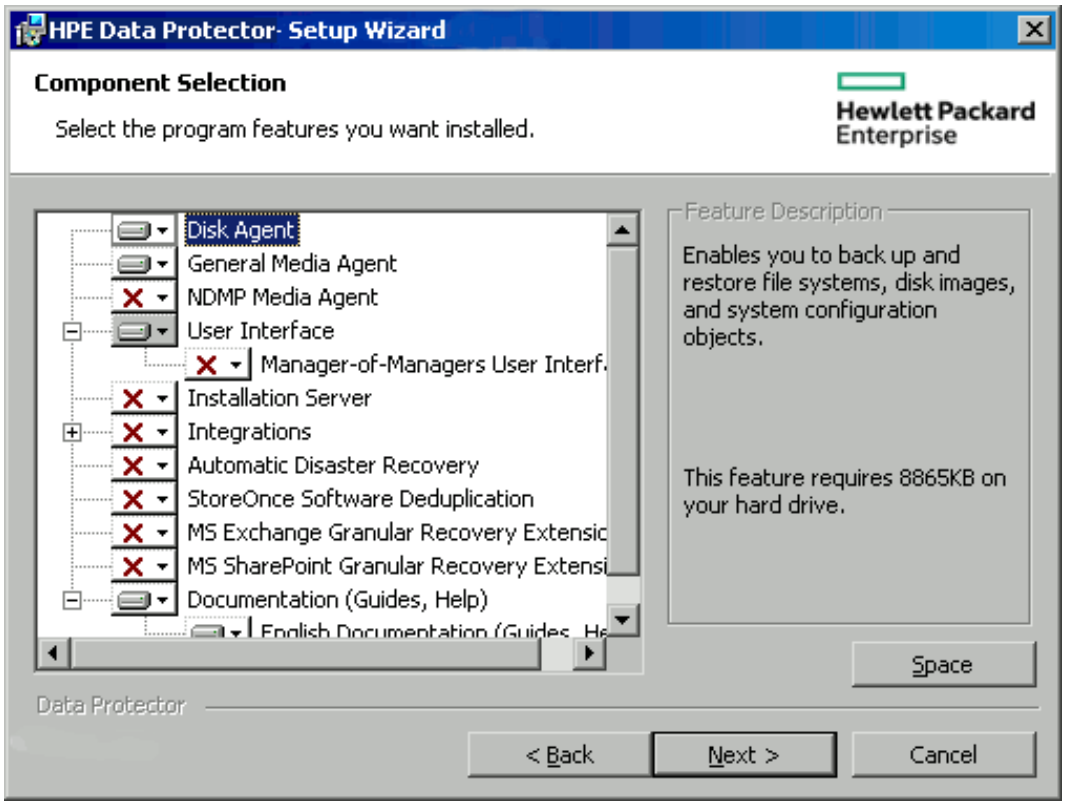
1. Copiez le package d'installation téléchargé sur un système Windows, et extrayez les fichiers vers un emplacement temporaire. Exécutez le fichier setup.exe que vous trouverez dans l'emplacement `\Windows_Other\x8664`. Il est recommandé de lancer l'installation sur le nœud de serveur virtuel actif.

L'installation détecte automatiquement la version précédente du produit et vous demande de la faire passer à .

Cliquez sur **Suivant** pour continuer.

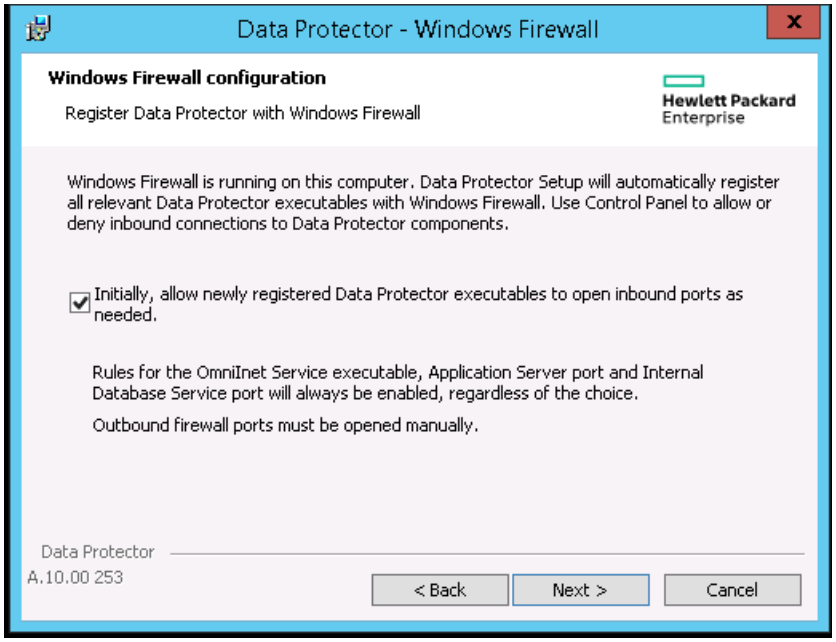
2. Data Protector détecte automatiquement les composants installés.

   Sélectionner les composants



   Cliquez sur **Suivant**.

3. Si Data Protector détecte Windows Firewall sur votre système, la page de configuration de Windows Firewall s'affiche. Le processus de configuration de Data Protector enregistre tous les exécutables Data Protector. 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 permettre à Data Protector d'ouvrir les ports pour le moment, ne cochez pas l'option. Pour un fonctionnement correct de Data Protector avec la version précédente des clients 10.00, les règles Data Protector dans le pare-feu Windows doivent être activées. Les règles pour l'exécutable du service OmniInet, le port du serveur d'application et le port de l'IDS seront toujours activées, indépendamment du choix effectué.



Cliquez sur **Suivant**.

4. Vous pouvez, si vous le souhaitez, modifier le compte utilisateur utilisé par l'IDB de Data Protector et HTTPS Application Server ainsi que les ports utilisés par ces services.

   Cliquez sur **Suivant**.

5. La liste des composants sélectionnés s'affiche. Cliquez sur **Installer** pour démarrer la mise à niveau.

   Une fenêtre d'invite de commande s'ouvre et le logiciel lance la migration IDB vers le nouveau format de base de données en exportant l'ancien IDB.

   Cette fenêtre reste ouverte pendant l'exportation de l'ancien IDB et affiche les messages de statut. L'exportation IDB peut nécessiter plusieurs minutes.

   Au cours de la mise à niveau, une nouvelle fenêtre d'invite de commande s'ouvre pour afficher le statut de l'importation des informations de configuration de l'IDB et des données dans Data Protector.

   Mises à niveau à partir des versions 8.00 et suivantes :

   L'IDB se met automatiquement à niveau, aucune fenêtre de commande ne s'ouvre.

   Après la mise à niveau, chaque nœud dispose des mêmes composants.

6. La page **État de l'installation** s'affiche. Cliquez sur **Suivant**.
7. Pour lancer le GUI Data Protector immédiatement après l'installation, sélectionnez **Lancer le GUI Data Protector**.

   Si le composant `English Documentation (Guides, Help)` a été mis à niveau ou récemment installé, pour voir les Annonces sur les produits, notes sur les logiciels et références Data Protector immédiatement après l'installation, sélectionnez **Références, notes de publication et annonces produits**.

   Cliquez sur **Terminer**.

REMARQUE :
Si vous mettez à niveau des clients en mode cluster, commencez par mettre à niveau chaque nœud de cluster séparément, puis importez à nouveau le serveur virtuel. Il n'est pas possible d'effectuer une mise à niveau à distance.

Migration des planifications depuis une ancienne version

Lorsque vous mettez à niveau vers Data Protector 10.00, toutes les planifications existantes migrent automatiquement vers le nouveau planificateur Web. Aucune intervention manuelle n'est nécessaire.

Au cours de la mise à niveau vers Data Protector 10.00, tous vos fichiers de planifications existantes sont dotés d'un suffixe `.migrate`.

Par exemple, dans les versions Data Protector antérieures à la version 10.00, si vous aviez une planification de spécification de sauvegarde appelée `WeeklyBackup`, le nom de fichier sera transformé en `WeeklyBackup.migrate` au cours de la mise à niveau. Si la migration échoue, les fichiers ne sont pas renommés.

Si les planifications ne migrent pas correctement, assistance clientèle vous demandera peut-être ces fichiers `.migrate` pour le dépannage.

Les fichiers de planification migrés sont disponibles dans l'emplacement suivant :

Type de spécification	Chemin d'accès de planification
Planifications de sauvegarde	Windows : *Data Protector_program_data*\OmniBack\Config\Server\amoschedules Unix : /var/opt/omni/server/amoschedules
Planifications d'intégration	Windows : *Data Protector_program_data*\OmniBack\Config\Server\Barschedules Unix : /var/opt/omni/server/Barschedules
Planifications d'opérations de copie	Windows : *Data Protector_program_data*\OmniBack\Config\Server\copylists\scheduled\schedules Unix : /var/opt/omni/server/copylists/scheduled/schedules
Planifications d'opérations de consolidation	Windows : *Data Protector_program_data*\OmniBack\Config\Server\consolidationlists\scheduled\schedules Unix : /var/opt/omni/server/consolidationlists/scheduled/schedules
Planification d'opérations de vérification	Windows : *Data Protector_program_data*\OmniBack\Config\Server\verificationlists\scheduled\schedules Unix :

	`/var/opt/omni/server/verificationlists/scheduled/schedules`
Planifications de groupe de rapports	Windows : *`Data Protector_program_data`*`\OmniBack\Config\Server\rptschedules` Unix : `/var/opt/omni/server/rptschedules`

Si la migration des planifications échoue au cours du processus de mise à niveau, vous pouvez exécuter manuellement la commande suivante pour réussir la migration des planifications existantes vers le nouveau planificateur :

```
omnidbutil -migrate_schedules
```

> **REMARQUE :**
> Les planifications ajoutées dans des versions antérieures de Data Protector n'avaient pas d'attribut de nom associé. Par conséquent, après la migration, le nom des planifications migrées apparaît comme **...**. Vous pouvez éditer ces planifications et leur donner un nom.

Chapitre 8: Data Protector Licensing

Ce chapitre contient des informations concernant :

- Présentation des nouvelles clés de licence
- Vérification et rapports de licences Data Protector
- Obtention et installation des mots de passe Data Protector
- Structure et licences de produit Data Protector

Aperçu

Vous devez avoir une clé de licence pour utiliser le produit Data Protector.

Data Protector obtient des licences (d'essai) immédiates dès la première installation.

Une licence d'essai est valide pendant 60 jours. Avant que la période de 60 jours n'expire, vous devez obtenir une licence permanente pour continuer d'utiliser Data Protector. Pour obtenir une licence permanente, consultez la section Obtention d'une licence, Page 291.

Ce chapitre explique les parties suivantes :

- Types de licences, bas : **licence basée sur les caractéristiques** est basée sur les caractéristiques et les cibles de sauvegarde. **Licence basée sur les capacités** est basée sur le volume de données sources originales protégées par Data Protector.
- Sélection du type de licence, Page 290 : cette partie explique les différences entre les licences basées sur les caractéristiques et les capacités. Les modèles de caractéristiques et de capacités peuvent être utilisés par le même client, mais ils ne peuvent pas être combinés sur le même Responsable de Cellule ou environnement MoM.
- Obtention d'une licence, Page 291 : cette partie fournit des détails sur l'obtention de nouvelles clés de licence et la demande de mots de passe.
- Gestion centralisée des licences, Page 299 : Data Protector vous permet de configurer la gestion centralisée des licences pour l'ensemble d'un environnement constitué de plusieurs cellules, ce qui simplifie la gestion de licence.
- Génération de rapports de licence, Page 300 : les licences Data Protector sont vérifiées et si elles sont absentes, elles sont signalées durant diverses opérations Data Protector.

Types de licences

Data Protector prend en charge deux schémas de licence :

- **Licence basée sur les caractéristiques** : basée sur les caractéristiques et les cibles de sauvegarde La licence basée sur les caractéristiques est également désignée licence traditionnelle.
- **Licence basée sur les capacités** : basée sur le volume des données source d'origine protégées par Data Protector. La capacité est mesurée en Téraoctets/TB Front End.

Licence basée sur les fonctionnalités

La structure du produit Data Protector et le modèle de licence basée sur les fonctionnalités consistent en trois catégories principales :

Licences liées au Cell Manager

- **Les Packs de démarrage :**

  Le pack de démarrage de Data Protector offre ce qui suit :

  - Un gestionnaire de cellule sur la plate-forme spécifiée (Windows, UNIX, Linux).
  - Un nombre illimité de clients de sauvegarde (agents) sur n'importe quelle plate-forme pour la sauvegarde du système de fichiers uniquement.
  - Une licence de lecteur (un lecteur de bande dans ce cas)
  - Des bibliothèques jusqu'à 60 logements
  - Options de reprise du système après sinistre
  - Des rapports de base (dans l'interface graphique de Data Protector et via le Web)

Cibles de sauvegarde

- **Extensions de lecteur et de bibliothèque :**
  - Extensions de lecteur de sauvegarde : inclut la licence pour la gestion d'un plus grand nombre de lecteurs en plus de celui disponible dans le pack de démarrage dans une cellule Data Protector
  - Extensions de bibliothèque : comprend la licence d'utilisation (LTU) pour la gestion des bibliothèques de bande avec le plus grand nombre de logements physiquement disponibles au sein d'une cellule Data Protector en plus de celui disponible avec le pack de démarrage.

La présence et le nombre des licences nécessaires basées sur entité est vérifié pour voir si l'un des éléments qui sont le sujet des licences basées sur la source est configuré dans la cellule. S'il y a moins de cellules que d'éléments configurés, Data Protector génère une notification.

Lorsqu'un périphérique de sauvegarde est configuré dans un environnement SAN pour plusieurs clients Data Protector, la fonctionnalité de chemins multiples doit être utilisée pour que Data Protector le reconnaisse comme un seul périphérique de sauvegarde.

Les cibles de sauvegarde suivantes sont sous licence par capacité :

- Sauvegarde sans temps d'indisponibilité UNIX pour 1 To et 10 To
- Sauvegarde sans temps d'indisponibilité UNIX baies non-HPE 1 To
- Récupération instantanée UNIX pour 1 To et 10 To
- Sauvegarde sans temps d'indisponibilité Linux pour 1 To et 10 To
- Sauvegarde sans temps d'indisponibilité Linux baies non-HPE 1 To
- Récupération instantanée Linux pour 1 To et 10 To
- Sauvegarde sans temps d'indisponibilité Windows pour 1 To et 10 To

- Sauvegarde sans temps d'indisponibilité Windows baies non-HPE 1 To
- Récupération instantanée Windows pour 1 To et 10 To
- Sauvegarde directe utilisant NDMP pour 1 To et 10 To
- Sauvegarde avancée vers disque pour 1 To,10 To et 100 To

Lorsqu'une licence pour une cible de sauvegarde qui est basée sur la capacité (autre que la sauvegarde avancée vers la licence de disque) est vérifiée, le volume de l'espace disque *total* sur des unités logiques qui ont été sauvegardées est comparé avec la capacité des licences installées. Pour la sauvegarde avancée vers la licence disque, voir La sauvegarde avancée vers la licence disque, Page suivante

La vérification de licence est effectuée de manière à ne pas vous empêcher de réaliser une récupération instantanée ou une sauvegarde même si vous manquez de capacité sous licence. Dans ces circonstances, un message d'avertissement apparaît au cours de la session de sauvegarde vous informant que vous avez excédé votre capacité sous licence.

La capacité des disques utilisés est calculée selon les informations historiques collectées au cours de chaque session de sauvegarde ZBD. L'intervalle de temps pris en compte est de vingt-quatre heures. Data Protector calcule la capacité des disques usagés en se basant sur les disques qui ont été utilisés dans toutes les sessions au cours des vingt-quatre dernières heures et compare la capacité calculée avec la capacité sous licence.

Si une violation de licence a lieu, un message d'avertissement est produit au cours de la sauvegarde. De plus, l'outil de reporting de licence est exécuté quotidiennement et écrit une notification dans le journal des événements de Data Protector si la capacité sous licence est excédée.

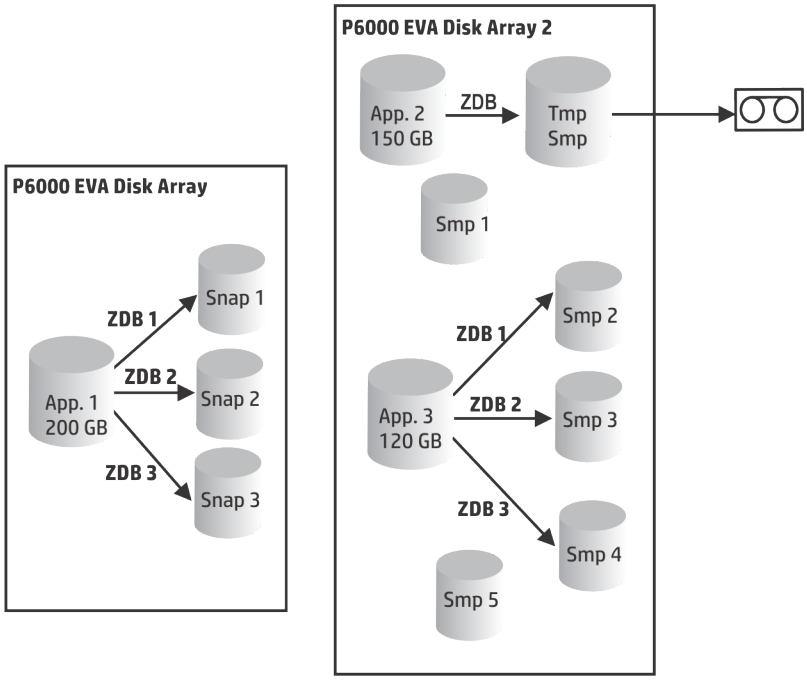
Calcul de capacité utilisée pour l'application des cibles de sauvegarde

Le calcul de capacité utilisée calcule la capacité sous licence de chaque baie de disque utilisée au cours des vingt-quatre dernières heures. Les disques utilisés deux fois ou plus dans l'intervalle de temps spécifié ne sont comptés qu'une seule fois. Les unités de baie de disque sont identifiés par leurs chiffres d'identification pris sur chaque baie . L'utilisation de chiffres d'identification de baie signifie qu'il est possible de savoir quand une baie a déjà été comptée.

Si une sauvegarde ZDB qui inclut la récupération instantanée a été lancée, la capacité totale de l'unité originale est calculée à la fois pour la capacité de ZDB utilisé par baie de disque, et en plus, pour la récupération instantanée par baie de disque.

Par exemple, supposons qu'il existe deux baies de disques P6000 EVA. Sur une baie se trouve un disque seul (App.1) avec une capacité de 200 Go utilisés par la protection de données. Les sessions de sauvegarde déclenchées trois fois par jour incluent une option de restauration instantanée. Trois répliques sont conservées simultanément. Elles sont utilisées tour à tour à des fins de restauration instantanée. Sur la deuxième baie de disque on trouve deux disques (App.2 et App.3) avec des capacités respectives de 150 Go et 120 Go. La sauvegarde est exécutée une fois par jour sur le disque App.2 et le snapshot est effacé après le déplacement des données sur la bande. Sur App.3 la sauvegarde est exécutée trois fois par jour et cinq répliques sont utilisées en rotation pour la restauration instantanée. Voir Scénario de calcul de capacité utilisée , Page suivante.

Scénario de calcul de capacité utilisée



Le calcul de la capacité utilisée par la ZDB compte tous les disques utilisés dans les sessions de sauvegarde au cours des dernières 24 heures : 200 GB (App.1) + 150 Go (App.2) + 120 Go (App.3) = 470 Go.

Les calculs de la capacité utilisée pour la restauration instantanée comptent la capacité source des sessions ZDB qui ont laissé des données à des fins de restauration instantanée. Le même disque est compté une fois seulement 200 Go (App.1) + 120 Go (App.3) = 320 Go.

La sauvegarde avancée vers la licence disque

La licence de sauvegarde avancée sur disque est requise pour effectuer une sauvegarde vers une bibliothèque de fichiers Data Protector. Elle peut aussi être utilisée pour une bibliothèque de bandes virtuelles (VTL) à la place des licences de lecteur.

- La capacité en natif utilisable d'une bibliothèque fichier de Data Protector est la taille de la bibliothèque fichier, comme signalée dans le système de fichiers.
  - Les sauvegardes complètes virtuelles et les sauvegardes incrémentales qui seront consolidées vers une sauvegarde complète ou virtuelle doivent être stockées dans la bibliothèque fichiers de Data Protector, qui nécessite cette licence.
- Si Data Protector utilise exclusivement VTL, il est recommandé de mettre sous licence une quantité correspondant à la capacité physique de VTL également connue comme la capacité en natif utilisable.
  - La capacité en natif utilisable de la bibliothèque de bande virtuelle (VTL) est la taille sur le disque de la bibliothèque de bande virtuelle consommée par toutes les sauvegardes protégées de Data Protector telles que signalées par la VTL.
  - Pour chaque VTL, vous pouvez choisir soit d'utiliser la sauvegarde vers le disque soit le modèle de licence de lecteur bande. Les deux concepts ne doivent pas être mélangés dans une VTL.

- Si la VTL dispose d'une possibilité intégrée de migrer les données sauvegardées depuis le cache du disque vers un autre disque ou une autre bande, la capacité de stockage migrée a besoin d'être pleinement sous licence. Aucune licence de lecteur ou de bibliothèque n'est nécessaire pour la bibliothèque de bande exclusivement contrôlée par la VTL, mais ***la capacité utilisée de toutes les bandes dans la bibliothèque de bande physique a besoin d'être sous licence***. Cependant, ce n'est pas applicable si la fonctionnalité de copie d'objet de Data Protector a été utilisée pour migrer les données sauvegardées vers un autre disque ou bande.

- Par défaut, Data Protector traite les périphériques VTL comme des bibliothèques ordinaires (telles que les bibliothèques SCSI II) et n'utilise pas la licence basée sur la capacité. Pour permettre la licence basée sur la capacité, le périphérique doit être marqué comme VTL au cours de la configuration du périphérique.

  Pour plus d'informations sur la manière de configurer une VTL via l'interface utilisateur graphique (GUI), reportez-vous à l'index *Aide de Data Protector* : "bibliothèque de bandes virtuelle" Pour plus d'informations sur la manière de configurer une VTL via l'interface ligne de commande (CLI), reportez-vous à la rubrique Exemple, bas suivante.

- Dans le cas d'une licence centrale avec Manager-of-Manager (MoM), vous avez besoin d'assigner au minimum 1 To à chaque cellule en utilisant la sauvegarde avancée vers la fonctionnalité disque.

> **REMARQUE :**
> Data Protector ne peut signaler le montant requis de licences en raison de l'instrumentation et des interfaces manquantes des VTL d'aujourd'hui et certains serveurs de fichiers accueillant la bibliothèque fichier de Data Protector. Il est de votre responsabilité de constamment mettre sous licence la capacité avec les définitions de licence.

Exemple

Si vous configurez une bibliothèque de bande virtuelle nommée "VTL_2011" via la ligne de commande (CLI) en utilisant la commande `omniupload`, vous devez spécifier la capacité estimée de la bibliothèque dans la configuration pour la chaîne `VTLCAPACITY`. La valeur estimée s'ajoute en conséquence à la capacité des licences utilisées pour la sauvegarde avancée vers disque dans le rapport de vérification de licence.

> **REMARQUE :**
> La valeur de consommation de capacité de la bibliothèque virtuelle estimée (`VTLCAPACITY`) en téraoctets (To) doit être un entier pour éviter le message d'erreur `Invalid VTL capacity specified`.

Dans le fichier de configuration nommé "libVTL.txt" dans le répertoire "C:\Temp" tapez la capacité de bibliothèque estimée, par exemple `11`, puis exécutez :

```
omniupload -create_library VTL_2011 -file C:\Temp\libVTL.txt
```

Pour vérifier la configuration de bibliothèque, exécutez :

```
omnidownload -library VTL_2011
```

```
#omnidownload -library VTL_2011
NAME "VTL2011"
DESCRIPTION ""
HOST computer.company.com
```

```
POLICY SCSI-II
TYPE DDS
LIBVIRTUAL
VTLCAPACITY 11
IOCTLSERIAL ""
CONTROL "SCSI address"
REPOSITORY
        "SCSI repository"
MGMTCONSOLEURL ""
```

Le vérificateur de licences fait un rapport sur la capacité en usage, qui est la somme de l'espace utilisé sur le disque pour la bibliothèque de fichier (FL) et la taille estimée de l'espace disque sur une bibliothèque de bande virtuelle. Par exemple, vous utilisez 2 To de l'espace disque en sauvegardant avec la FL et 10 To de la capacité disque sur la VTL. La capacité totale en utilisation est de 12 To. S'il n'y a que 5 To de capacité de licences installées, vous recevez une notification vous indiquant que vous avez besoin de 7 licences supplémentaires de sauvegarde avancée vers le disque pour 1 To.

```
#omnicc –check_licenses –detail
------------------------------------------------------------
Catégorie de licences          : 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
Total protected data        1 TB
```

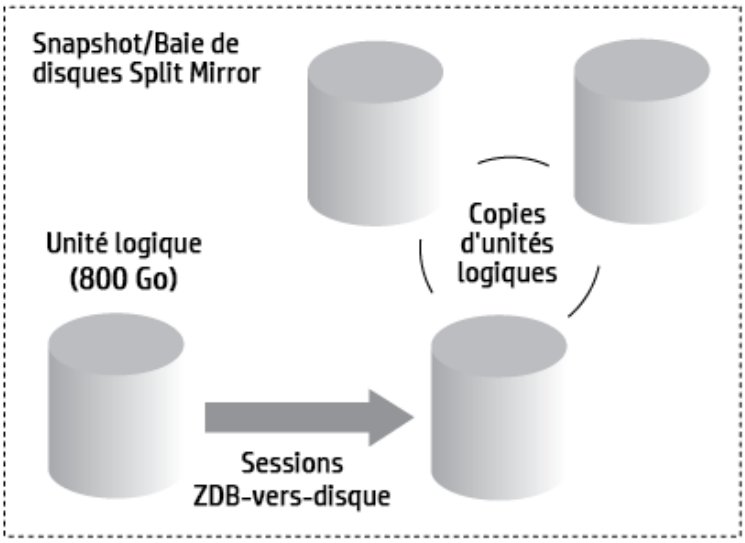
Exemples de cibles de sauvegarde basées sur la capacité sous licence

Cette section fournit des exemples sur la manière dont est calculée la licence basée sur la capacité.

Exemple 1

La rubrique Sessions ZDB-vers-disque , Page suivante montre une situation dans laquelle les données d'une unité logique de 800 Go est sauvegardée trois fois par jour dans une session ZDB-vers-disque.

Sessions ZDB-vers-disque



Trois copies Split Mirror ou Snapshot sont mises en rotation et conservées en prévision d'une restauration instantanée. La licence basée sur la capacité est calculée comme suit :

Une unité logique de 800 Go est utilisée pour les sessions de sauvegarde avec temps d'indisponibilité nul sur disque :

1 x 800 Go = 0,8 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

Trois répliques de la même unité logique de 800 Go sont conservées en prévision d'une restauration instantanée. Notez que la licence s'applique à la capacité des volumes sources, et non à la capacité des répliques :

1 x 800 Go = 0,8 To pour la licence "Restauration instantanée pour 1 To".

Dans cet exemple, une licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To" et une licence "Restauration instantanée pour 1 To" suffisent.

Exemple 2

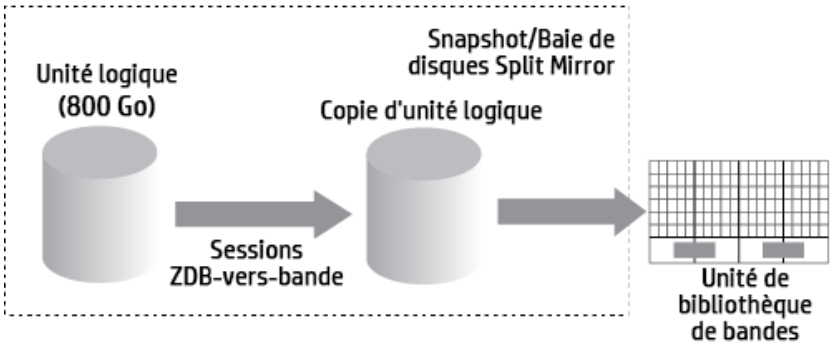
La rubrique Sessions ZDB-vers-bande , Page suivante montre une situation dans laquelle les données d'une unité logique de 800 Go est sauvegardée deux fois par jour dans une session ZDB-vers-bande. En conséquence, trois copies Split Mirror ou Snapshot ne sont pas conservées en prévision d'une restauration instantanée. La licence basée sur la capacité est calculée comme suit :

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".

Une seule licence Sauvegarde avec temps d'indisponibilité nul pour 1 To suffit.

Sessions ZDB-vers-bande



Exemple 3

La rubrique Sessions ZDB-vers-disque+bande, bas montre une situation dans laquelle les données d'une unité logique de 800 Go est sauvegardée trois fois par jour dans une session ZDB-vers-disque+bande. Cinq versions Split Mirror ou de répliques sont mises en rotation et conservées en prévision d'une restauration instantanée. La licence basée sur la capacité est calculée comme suit :

Une unité logique de 800 Go est utilisée pour les sessions ZDB sur disque + bande :

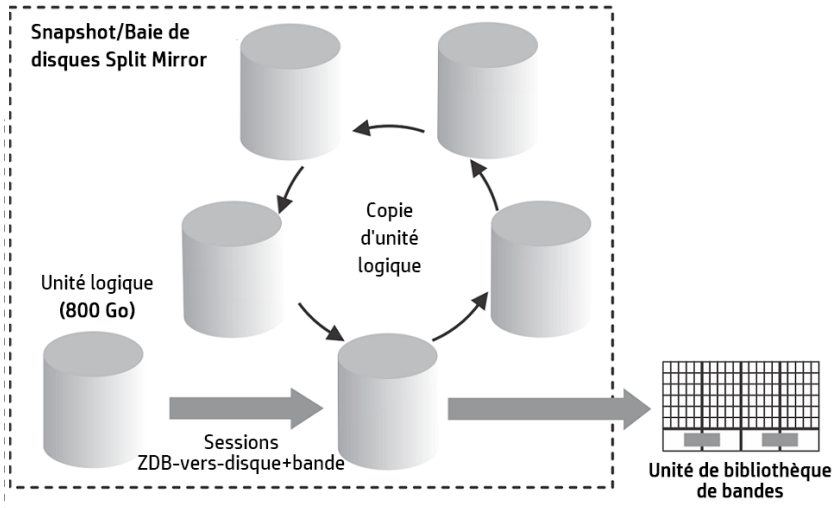
1 x 800 Go = 0,8 To pour la licence "Sauvegarde avec temps d'indisponibilité nul pour 1 To".

Cinq répliques de la même unité logique de 800 Go sont conservées en prévision d'une restauration instantanée. Notez que la licence s'applique à la capacité des volumes sources, et non à 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.

Sessions ZDB-vers-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 ZDB :

1 x 200 Go + 1 x 500 Go + 1 x 120 Go + 1 x 300 Go = 1,12 To pour la licence "Sauvegarde à temps d'indisponibilité nul pour 1 To".

Des copies Split Mirror ou Snapshot d'unités logiques de respectivement 200 Go, 120 Go et 300 Go sont conservées à des fins de restauration instantanée :

1 x 200 Go + 1 x 120 Go + 1 x 300 Go = 0,62 To pour la licence "Restauration instantanée pour 1 To".

Une licence "Sauvegarde à temps d'indisponibilité nul pour 1 To" et une licence "Restauration instantanée pour 1 To" suffisent si les trois exemples de Sessions ZDB-vers-disque , Page 285 à Sessions ZDB-vers-disque+bande, Page précédente sont configurés dans une cellule.

Extensions de fonctionnalités :

- Sauvegarde en ligne : la possibilité de sauvegarder des serveurs d'application et des environnements virtuels lorsque l'application est en cours d'exécution.
- Extension en ligne pour un système UNIX et extension en ligne pour un système Windows / Linux.
- La fonctionnalité Manager-of-Managers.
- Bibliothèques avec plus de 60 emplacements.
- Extension de cryptage de Data Protector pour un système client
- Sauvegarde NDMP.
- Extension de récupération granulaire pour un serveur de base de données.
- Sauvegarde avec temps d'indisponibilité nul (ZDB) : la possibilité de sauvegarder des instantanés basés sur une baie pour les systèmes de stockage HP.
- Restauration instantanée (IR) : permet de restaurer la sauvegarde créée à partir d'un instantané basé sur une baie.
- Sauvegarde avancée sur disque : inclut la licence pour 1 To de stockage sur disque de sauvegarde. Capacité en natif utilisable de stockage de sauvegarde disque requise une fois par téraoctet (To). La licence est requise pour la sauvegarde dans une bibliothèque de fichiers Data Protector et une sauvegarde Data Protector vers un type de périphérique à disque, et peut être utilisée au lieu de licences de lecteur pour sauvegarder sur une bibliothèque de bande virtuelle.

Licence basée sur la capacité

La structure de produit basée sur la capacité est basée sur le volume de données primaires protégées par Data Protector et inclut l'utilisation illimitée des caractéristiques de protection de l'entreprise. La capacité est mesurée dans "Téraoctets Front End" ou Front End To. Le volume total des Téraoctets Front End est défini comme le volume agrégé de données de tous les systèmes en cours de sauvegarde dans le Gestionnaire de cellule. Il est mesuré par système comme le plus grand et complet (c'est-à-dire, le volume des données source protégées). Ce modèle de licence peut être appliqué à l'infrastructure existante. La nouvelle infrastructure est automatiquement incluse dans la même licence.

CBL inclut toutes les données protégées dans le calcul et ne peut pas faire la distinction entre le type de licence (actuelle/d'origine) utilisé pour la sauvegarde. Les systèmes qui ne sont pas inclus dans la

sauvegarde (qui n'existent plus) peuvent être copiés sr un média séparé qui peut être exporté depuis le système Gestionnaire de cellule.

> **REMARQUE :**
> Les objets IDB ne sont pas inclus dans le calcul CBL.

Lors de l'utilisation de la gestion de licence basée sur la capacité, les modules suivants font partie de la structure de licence :

- Gestionnaires de cellule et Manager of Managers
- Lecteurs bandes et bibliothèques
- Sauvegarde en ligne et Extensions de récupération granulaire
- Sauvegardes sans temps d'indisponibilité et Récupération instantanée
- Sauvegarde avancée vers disque et NDMP

Les produits non inclus et vendus séparément des licences basées sur la capacité comprennent :

- Les logiciels de chiffrement
- Navigateur de sauvegarde
- Optimiseur de stockage
- Sauvegarde en ligne étendue DP
- Sauvegarde avec temps d'indisponibilité nul de Data Protector pour les baies hors HPE
- Pack de gestion Data Protector comprenant le plug-in DP Smart pour le Gestionnaire des opérations et Microsoft Systems Center

Consultez les spécifications de Data Protector pour connaître les niveaux de capacité, leur description et les numéros de pièce..

Rapports de licence basée sur la capacité

Dans le mode de licence basée sur la capacité, Data Protector liste uniquement le nombre de licences basées sur la capacité (avec une granularité de 1 To) et les licences qui ne sont pas couvertes par les licences basées sur la capacité, c'est-à-dire l'extension de Cryptage Logiciel. Les licences basées sur les fonctionnalités qui sont couvertes par la licence basée sur la capacité ne sont pas affichées.

```
#omnicc -check_license -detail

AVERTISSEMENT : le calcul de la taille totale des données protégées peut prendre un
certain temps.

Rapport généré                          : 10/12/2013 1:48:27 AM
Mode d’attribution de licence           : Serveur
Serveur de licences                     : hote.domaine.com
-------------------------------------------------------------------------------
---
Catégorie de licences               : Extension de cryptage pour un système client
Licences installées                 : 0
Licences utilisées                  : 0
Licences supplémentaires requises   : 0
-------------------------------------------------------------------------------
---
```

```
Catégorie de licences                 : Data Protector - basée sur la capacité en
To SW
Capacité de licences installées       : 9 To
Capacité de licences utilisées        : 0 To
Ajouter. Capacité de licences requises : 0 To
-------------------------------------------------------------------------------
---
.
.
.

Résumé
-------
La gestion de licence est couverte.
Données totales protégées       : 4,00 To

-------------------------------------------------------------------------------
---
Type de sauvegarde                                    |       Données totales protégées
-------------------------------------------------------------------------------
---

MS Filesystem                                 |       1 Go
MS SQL                                        |       1 Go
SAP                                           |       1 Go
UNIX Filesystem                               |       1 Go

-------------------------------------------------------------------------------
```

La totalité des données protégées se définit comme la quantité cumulée des données sauvegardées depuis l'ensemble des systèmes. La totalité des données protégées pour chaque système est calculée comme étant la somme des éléments suivants :

- Somme de la sauvegarde complète la plus volumineuse de chaque objet du système de fichiers (y compris les sauvegardes synthétiques) et des sauvegardes d'environnement virtuel.
- Somme de la sauvegarde complète la plus volumineuse de chaque ensemble de données pour chacune des sauvegardes d'intégration d'application.

> **REMARQUE :**
> L'objet unique pour chacun des systèmes de fichiers et des environnements virtuels correspond à l'objet réel créé au moment de la sauvegarde. L'objet réel peut être soit un point de montage, soit une machine virtuelle, soit un disque de machine virtuelle.
>
> L'ensemble de données unique pour chacune des intégrations d'application est identifiée différemment : en règle générale, il s'agit du nom de l'instance de base de données ou du serveur.

Limites

- Lors de la sauvegarde de données identiques avec plusieurs agents différents, la sauvegarde est calculée plusieurs fois. Voici quelques exemples de calculs en double :

- Sauvegarde du système de fichiers de la base de données à l'aide de VSS et sauvegarde de l'agent d'intégration d'application de la même base de données.
- Sauvegarde de l'intégration d'environnement virtuel de l'hôte virtuel et sauvegarde de l'agent du système de fichiers exécuté à l'intérieur de la machine virtuelle (hôte).

> **REMARQUE :**
> Il est recommandé de sauvegarder des objets uniques afin d'éviter les doublons lors des calculs.

- Lorsque le format du nom d'objet de sauvegarde Oracle est reconfiguré en externe, il peut en résulter une absence de résolution du nom de la base de données à partir des nouveaux noms d'objet. Ces tailles d'objet peuvent être traitées de façon incorrecte lors du calcul du total des données protégées.

> **REMARQUE :**
> Il est essentiel qu'un format reconfiguré inclue le nom de la base de données Oracle défini comme `<DBID_*.dbf` pour que l'ajout des objets Oracle dans le calcul de la taille du total des données protégées soit correct.

- Il n'existe actuellement aucun moyen dans Data Protector de détecter si la machine virtuelle VMWare sauvegardée avec l'agent d'environnement virtuel et par l'agent de disque installé qui s'exécute à l'intérieur de la machine virtuelle, VEPA et l'agent de disque s'exécutent sur les mêmes données.

Sélection du type de licence

Les modèles basés sur les fonctionnalités et sur la capacité peuvent être utilisés par le même client, mais ils ne peuvent pas être associés sur le même Gestionnaire de cellule ou environnement MoM. Les produits complémentaires répertoriés sont l'exception à cette règle, car ces licences peuvent être combinées avec les méthodes de gestion des licences basées sur les fonctionnalités et sur la capacité de Data Protector. La migration d'une structure de produit traditionnelle à une autre basée sur la capacité est prise en charge. Contactez votre représentant autorisé Hewlett Packard Enterprise pour plus de détails. Les deux modèles de licence sont valides pour toute taille d'environnement.

Les différences entre les licences basées sur les fonctionnalités et sur la capacité sont les suivantes :

- Les licences basées sur les fonctionnalités offrent un coût d'entrée plus abordable, avec moins de fonctionnalités activées, là ou les licences de capacité offrent de nombreuses fonctionnalités et un modèle de paiement évoluant avec votre croissance.
- Le modèle de licence basée sur les fonctionnalités nécessite une licence distincte pour chaque gestionnaire de cellule, lecteur de bande, etc. et exige que les utilisateurs documentent d'abord leur environnement existant puis choisissent les fonctionnalités logicielles de sauvegarde pour lesquels ils ont besoin d'une licence pour protéger leur environnement.
- Plus de souplesse : le modèle de licence basée sur la capacité nécessite une licence pour protéger le volume total des données sur les clients ayant besoin de protection.
- Un autre problème possible est si vous conservez vos données pendant une longue période de temps, et que les données changent significativement sans pour autant augmenter en capacité. Dans ce cas, ce modèle alternatif basé sur la capacité pourrait coûter plus cher avec le temps.

Pourquoi utiliser une licence basée sur les fonctionnalités ?

- Ces licences offrent un coût d'entrée inférieur avec moins de fonctionnalités activées
- Si les données de l'organisation augmentent constamment à un taux raisonnable, il peut être plus rentable d'utiliser la méthode de licence basée sur les fonctionnalités

Pourquoi utiliser une licence basée sur la capacité ?

- Ces licences sont basées sur la quantité de données de production protégées par Data Protector
- Elles permettent d'effectuer plusieurs copies sans augmentation des coûts de licence
- Elles offrent une utilisation illimitée des fonctionnalités de protection d'entreprise
- Elles sont perpétuelles et peuvent être transférées vers de nouveaux serveurs, stockages, applications, etc.
- Elles offrent un système de paiement à la croissance évolutif et abordable pour une meilleure gestion des coûts d'exploitation et un dimensionnement simplifié

Obtention d'une licence

Cette section fournit des informations sur l'obtention de nouvelles clés de licence et la demande de nouveaux mots de passe pour les clés existantes pour Data Protector.

Obtention de nouvelles clés de licence

Les clés de licence et les mots de passe générés dans Data Protector 8.00 et sur les versions antérieures avant doivent être mis à jour, car ils ne sont pas compatibles avec la dernière version de Data Protector en raison de changements dans les technologies de licence.

Les clés de licence et les mots de passe générés avant Data Protector 10.00 ne sont pas compatibles avec Data Protector 10.00 et ultérieur. De nouvelles licences sont requises pour mettre à jour vers Data Protector 10.00.

> **REMARQUE :**
> Data Protector 10.00 n'affiche plus les licences expirées ou invalides.

En ce qui concerne les licences récemment achetées, vous devez sélectionner la version de produit Data Protector 10.00 lors de la demande d'un mot de passe. Un mot de passe généré pour Data Protector 10.00 ne fonctionnera pas avec une version précédente de Data Protector.

Apres la mise a jour, Data Protector 10.00 s'exécutera avec un mot de passe Instant-On de 60 jours. Le comportement sera identique à une installation nouvelle avec un mot de passe Instant-On.

> **IMPORTANT :**
> Dès qu'*au moins une nouvelle clé de licence* pour Data Protector 10.00 a été installée, le mot de passe Instant-On sera désactivé et seules les clés valides installées seront reconnues.

L'activation des mots de passe instant-on après la mise à jour ne peut être effectuée qu'une seule fois.

> **CONSEIL :**
> Après la mise à jour, les licences existantes sont encore reportées comme invalides en même

temps que les nouvelles (Instant-On). Pour éviter cela, renommez (mais n'effacez pas) le fichier `lic.dat` :

Systèmes Windows : Accédez au répertoire *`Data_Protector_program_data`*`\Config\server\Cell` et renommez le fichier :

```
ren lic.dat lic.bak
```

Systèmes UNIX **:** Accédez au répertoire `/etc/opt/omni/server/cell` et déplacez le fichier :

```
mv lic.dat lic.bak
```

Considérations relatives aux mots de passe

Considérez les éléments suivants pour aider à déterminer le bon nombre de mots de passe :

- Les mots de passe Instant-On sont intégrés. Ils sont disponibles pour chaque nouvelle installation et chaque installation existante de Data Protector mise à jour vers la version Data Protector 9.00 ou ultérieure pendant 60 jours sans autre exigence d'installation de licence de mot de passe supplémentaire, et ils vous offrent la fonctionnalité complète du produit à des fins d'évaluation.

  Après 60 jours, les mots de passe instant-On expirent et le produit cesse de fonctionner, à moins qu'une clé de licence permanente ait été installée.

  La période d'installation pour le produit complet se termine dès que la clé de licence normale est installée. Dès qu'au moins une clé de licence est installée, seule la fonctionnalité peut être utilisée, pour laquelle les clés de licence ont été installées.
- Les licences permanentes peuvent être déplacées vers un Gestionnaire de cellule différent. Toutefois, vous devez utiliser le(s) formulaire(s) de déplacement de licence et le(s) envoyer au Centre de délivrance de mot de passe.
- Les mots de passe sont installés sur le Gestionnaire de cellule et valables pour toute la cellule.
- La licence centralisée est fournie dans la fonctionnalité de Manager-of-Managers (MoM). Vous pouvez installer toutes les licences sur le système MoM si vous achetez des licences multiples pour plusieurs cellules.
- Vous avez besoin d'une licence de Gestionnaire de cellule pour chaque cellule.
- Les clés de licence ou mots de passe sont régulièrement vérifiés par le logiciel lorsque vous effectuez une mission de configuration de Data Protector ou démarrez une session de sauvegarde.
- Les mots de passe Instant-On peuvent être utilisés sur tout système, tandis que les mots de passe d'évaluation et permanents ne peuvent être utilisés que pour le système du Gestionnaire de cellule pour lequel vous avez demandé les licences.

La licence de Data Protector nécessite un des mots de passe suivants :

- Mot de passe Instant-On

  Un mot de passe Instant-On est intégré dans le produit à la première installation. Vous pouvez utiliser le logiciel pendant 60 jours après l'avoir installé sur tout système pris en charge par Data Protector. Au cours de cette période vous devez demander votre mot de passe permanent au *Centre de délivrance de mot de passe (PDC)* puis l'installer.

  Pour une installation existante de Data Protector, apres la mise a jour vers ou ultérieur, Data Protector9.00votre installation est lancée avec un mot de passe Instant-On pendant 60 jours. Au cours de cette période, vous devez demander vos nouveaux mots de passe permanents au Centre

de livraison de mot de passe comme spécifié dans votre accord d'assistance active. Les anciennes licences qui ne sont pas couvertes dans l'accord d'assistance ne peuvent être mises à jour.

- Mots de passe permanents

  Le produit Data Protector est distribué avec une licence *de Certificat* qui vous donne le droit d'obtenir un mot de passe permanent. Le mot de passe permanent vous permet de configurer une cellule Data Protector en relation avec votre stratégie de sauvegarde, dans la mesure où vous avez acheté les licences nécessaires. Avant de demander un mot de passe permanent, vous devez déterminer le système Gestionnaire de cellule et comprendre les exigences de configuration de votre cellule.

- Mot de passe d'urgence

  Les mots de passe d'urgence ou de repli sont disponibles au cas où les mots de passe actuellement installés ne correspondent pas avec la configuration système actuelle en raison d'une urgence. Ils permettront le fonctionnement sur tout système pour une durée de 120 jours.

  Les mots de passe d'urgence sont produits par l'organisation d'assistance. Ils doivent être demandés par et sont produits uniquement pour le votre représentant assistance clientèle. Référez-vous a votre contact d'assistance ou consultez le site de licence de a : https://software.microfocus.com/fr-fr/legal/software-licensing.

  La finalité d'un mot de passe d'urgence est de permettre le fonctionnement d'une opération de sauvegarde tandis que la configuration système est reconstruite ou jusqu'à que vous effectuiez une nouvelle installation permanente. Dans le cas ou vous déplacez les licences, vous devez remplir le Formulaire de déplacement de licence et l'envoyer *au Centre de délivrance de mot de passe (PDC) ou rendez-vous sur la page web* https://software.microfocus.com/fr-fr/legal/software-licensing ou les mots de passe peuvent etre générés, et ainsi de suite.

Pour les instructions sur la façon d'obtenir et d'installer un mot de passe, voir Obtention de mots de passe permanents, bas.

Obtention de mots de passe permanents

Voici les procédures pour obtenir des mots de passe permanents :

1. Rassemble les informations nécessaires dans le *Formulaire de demande* de mot de passe permanent. Reportez-vous à Formulaires de licence Data Protector, Page 295 pour trouver l'emplacement des formulaires et obtenir les instructions sur la manière de les remplir.
2. Le *Centre de délivrance de mot de passe* vous enverra votre mot de passe permanent en utilisant le même moyen que celui que vous avez utilisé lorsque vous avez envoyé votre demande. Par exemple, si vous envoyez une requête par e-mail alors vous recevrez votre mot de passe permanent par e-mail.
3. Effectuez l'une des actions suivantes :
   - Rendez-vous sur le site en ligne du *Centre de délivrance de mot de passe* à l'adresse https://software.microfocus.com/fr-fr/legal/software-licensing.
   - Remplissez le *Formulaire de demande de mot de passe permanent* et envoyez-le au *Centre de délivrance de mot de passe* en utilisant un des éléments suivants (reportez-vous au Certificat envoyé avec le produit pour les numéros de fax, de téléphone, adresses e-mail et heures d'ouverture) :
     - Faxer un formulaire au *Centre de délivrance de mot de passe*
     - Envoyer un e-mail au *Centre de délivrance de mot de passe*

Vous pouvez utiliser la version électronique des formulaires de licence qui sont inclus dans les fichiers suivants sur le Gestionnaire de cellule et le support d'installation :

Sur Windows Gestionnaire de cellule :`répertoire_Data_Protector\Docs\license_forms.txt`

Sur UNIX Gestionnaire de cellule :`/opt/omni/doc/C/license_forms_UNIX`

Dans le package d'installation Windows :`\Docs\license_forms.txt`

pour “copier” et “coller” votre message au Centre de délivrance de mot de passe *(PDC)*.

Vous recevrez votre mot de passe permanent dans les 24 heures suivant l'envoi de votre *Formulaire de demande de mot de passe permanent*.

Installation des mots de passe permanents

Cette section décrit la procédure pour installer un mot de passe permanent que le *Centre de délivrance de mot de passe (PDC)* vous a envoyé.

Conditions préalables :

Vous devez avoir reçu le mot de passe permanent envoyé par le *Centre de délivrance de mot de passe* et l'interface utilisateur Data Protector doit être installée sur le Gestionnaire de cellule. Les mots de passe sont installés sur le Gestionnaire de cellule et sont valides pour toute la cellule.

Utilisation de l'interface utilisateur graphique :

Pour installer le mot de passe permanent en utilisant l'interface graphique utilisateur de Data Protector, procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, faites un clic droit sur **Data Protector Cellule** puis cliquez sur **Ajouter licence**.
3. Indiquez ou copiez le mot de passe exactement tel qu'il figure sur le *Certificat de mot de passe*.

   Un mot de passe se compose de 4 groupes de caractères de longueur variable, 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 :

   ```
   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR
   KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK
   ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX
   ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "Product; Cell Manager for UNIX"
   ```

   Une fois le mot de passe indiqué, vérifiez les points suivants :

   - 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 en fin du mot de passe, ni de caractères en trop.
   - Vérifiez que vous n'avez pas confondu les caractères "1" (chiffre un) et "l" (lettre l).
   - Vérifiez que vous n'avez pas confondu les caractères "O" (lettre majuscule) et "0" (chiffre).

- Vérifiez que vous avez utilisé la bonne casse. La casse du mot de passe est prise en compte.

Cliquez sur **OK**.

Le mot de passe est écrit dans le fichier suivant sur le Gestionnaire de cellule :

Systèmes Windows :*données_programme_Data_Protector*\Config\server\Cell\lic.dat

Systèmes UNIX :/etc/opt/omni/server/cell/lic.dat

Utilisation de l'interface de ligne de commande :

Pour installer le mot de passe permanent en utilisant le CLI de Data Protector, procédez comme suit :

1. Identifiez-vous sur Gestionnaire de cellule.
2. Exécuter la commande suivante :

   omnicc -install_license *password*

   La chaîne *password* doit être saisie exactement telle qu'elle apparaît sur le *Certificat de mot de passe*. Il doit être formaté comme une ligne seule et ne doit pas contenir de retour à la ligne intégré. Le mot de passe doit être entre guillemets. Si le mot de passe inclut également une description entre guillemets, les guillemets dans cette description doivent être précédés de barres obliques inversées. Pour un exemple et plus d'informations, reportez-vous à la page man omnicc ou au *Guide de référence de l'interface de ligne de commande Data Protector*.

Vous pouvez également ajouter le mot de passe au fichier suivant sur le Gestionnaire de cellule:

Systèmes Windows :*données_programme_Data_Protector*\config\server\cell\lic.dat

Systèmes UNIX :/etc/opt/omni/server/cell/lic.dat

Si le fichier n'existe pas, créez-le avec un éditeur, tel que vi ou Notepad. Pour un exemple de mot de passe, voir Indiquez ou copiez le mot de passe exactement tel qu'il figure sur le Certificat de mot de passe., Page précédente dans la procédure pour l'interface graphique utilisateur.

Formulaires de licence Data Protector

Cette section présente les Data Protector formulaires de licence. Remplissez-les pour commander des mots de passe permanents en utilisant un des moyens suivants :

- Commandez des mots de passe permanents en utilisant le site du *Centre de délivrance de mot de passe* en ligne à l'adresse https://software.microfocus.com/fr-fr/legal/software-licensing.
- Imprimez la version électronique des formulaires de licence qui sont inclus dans les fichiers suivants sur le système Gestionnaire de cellule et le support d'installation :

  Systèmes HP-UX et Linux :/opt/omni/doc/C/license_forms_UNIX

  Package d'installation Windows :Docs\license_forms.txt

  ou utilisez les fichiers électroniques pour “copier” et “coller” votre message au *Centre de délivrance de mot de passe (PDC)*.

> **IMPORTANT :**
> Assurez-vous de saisir clairement les informations et que vous n'oubliez pas les champs obligatoires.

Les champs généraux dans les formulaires de licence que vous devez remplir sont brièvement décrits en dessous :

Données personnelles	Ce champ contient les informations client, comprenant la personne à qui le nouveau mot de passe doit être délivré.
Données de licence	Fournissez les informations de licence à propos de votre cellule Data Protector.
Gestionnaire de cellule actuel	Fournissez les informations nécessaires concernant l'actuel Gestionnaire de cellule.
Nouveau Gestionnaire de cellule	Fournissez les informations nécessaires concernant votre nouveau Gestionnaire de cellule.
Numéro de commande	Saisissez le *Numéro de commande* imprimé sur le *Certificat.* Le *Numéro de commande* est nécessaire pour vérifier que vous êtes en droit de demander un mot de passe permanent.
Adresse IP	Ce champ définit le système pour lequel le *Centre de délivrance de mot de passe* générera les mots de passe. Au cas où vous voulez utiliser la gestion de licence centralisée (environnement MoM uniquement) alors ce système doit être le système de Gestionnaire MoM. Si le Gestionnaire de cellule dispose de plusieurs cartes LAN, vous pouvez saisir n'importe laquelle des adresses IP. Micro Focus recommande que vous saisissiez la première. Si vous avez Data Protector dans un environnement Serviceguard ou Microsoft Cluster, saisissez l'adresse IP de votre serveur virtuel. Pour plus d'informations sur les clusters, reportez-vous au *Aide de Data Protector*.
Les numéros de fax du *Centre de délivrance de mot de passe*	Pour des informations de contact, reportez-vous au *Certificat* distribué avec votre produit.
Type de licence produit	Dans les champs près des *Numéros de produit*, saisissez la quantité de licences que vous voulez installer sur ce Gestionnaire de cellule. La quantité peut être la totalité ou bien un sous-ensemble des licences achetées avec le *Numéro de commande*.

Vérification du mot de passe

Utilisation de l'interface utilisateur graphique

Pour vérifier si 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 **Licences**.
2. Cliquez sur l'onglet **Licences**. Toutes les licences installées sont affichées. Cliquez sur l'onglet **Infos mots de passe** pour voir les détails sur les mots de passe valides installés. Les mots de

passe invalides seront marqués comme expirés ou supprimés.

Toute la fenêtre pop-up ainsi que les colonnes individuelles sont redimensionnables.

Utilisation de l'interface de ligne de commande

Pour vérifier si le mot de passe pour la licence que vous avez installée est correct, utilisez la commande suivante :

```
omnicc -password_info
```

Cette commande affiche les licences installées. Si le mot de passe saisi est incorrect, il est listé avec la remarque `Password could not be decoded.`

Trouver le nombre de licences installées

Utilisation de l'interface utilisateur graphique

Une fois que vous avez installé un mot de passe permanent, vous pouvez vérifier le nombre de licences installées sur le Gestionnaire de cellule:

1. Démarrez Data Protector Manager.
2. Dans la barre du menu, cliquez sur **Aide**, puis **Licences...**. La fenêtre A propos de Manager s'ouvrira, affichant les licences installées.

Utilisation de l'interface de ligne de commande

Si vous utilisez la ligne de commande, procédez comme suit :

1. Identifiez-vous sur Gestionnaire de cellule.
2. Exécuter la commande suivante :

   ```
   omnicc -query
   ```

Un tableau listant les licences actuellement installées s'affichera.

Mise à niveau de licences existantes

Si vous êtes un client Data Protector existant, afin de mettre à jour vos anciens mots de passe de licence vers la version la plus récente de Data Protector, vous devez avoir un accord de prise en charge active mis en place, couvrant la qualité et les types de licence que vous pouvez utiliser.

Une fois que vous avez reçu les nouvelles clés de licence, comparez-les à la quantité et au type de clés de licence installées dans votre environnement Data Protector. Ne mettez à jour le logiciel qu'après avoir vérifié que vous êtes en possession de suffisamment de clés de licences valides basées sur .

Si vous avez reçu un nombre de nouvelles clés de licence inférieur au nombre effectivement installé dans votre environnement Data Protector, ou des clés différentes, n'effectuez pas la mise à vers la dernière version de Data Protector. Il existe sinon un risque que votre environnement Data Protector ne soit plus fonctionnel en raison des clés de licence manquantes.

Vous devriez au contraire d'abord contacter votre représentant des ventes ou votre partenaire pour déterminer quelles étapes sont à suivre pour réduire l'écart dans la couverture de fonctionnalité

licenciée par votre contrat d'assistance et les licences actuelles en usage avec les versions de Data Protector précédant Data Protector10.00.

Une fois que vous avez installé le produit Data Protector, vous pouvez commencer à l'utiliser pendant 60 jours. Après cette période, vous devez installer un mot de passe permanent sur le Gestionnaire de cellule pour activer le logiciel. Vous pouvez charger le logiciel sur le Data ProtectorGestionnaire de cellule, mais vous ne pouvez pas effectuer de tâches de configuration sans un mot de passe permanent, car les licences requises pour la fonctionnalité Data Protector particulière nécessitent des mots de passe.

Déplacer les licences vers un autre systemeGestionnaire de cellule

Vous devez contacter le *Centre de délivrance de mot de passe* dans tous les cas suivants :

- Si vous souhaitez déplacer le Gestionnaire de cellule vers un autre système.
- Si vous prévoyez de déplacer une licence, installée sur un Gestionnaire de cellulequi n'est pas utilisé actuellement dans la cellule, vers une autre cellule Data Protector.

> **REMARQUE :**
> Les licences de produit UNIX fonctionnent sur les plates-formes UNIX, Windows, et Novell NetWare, fournissant la fonctionnalité quelle que soit la plate-forme, tandis que les licences de produit Windows fonctionnent uniquement sur les plates-formes Windows, Novell NetWare et Linux.
>
> Une licence de Gestionnaire de cellule pour HP-UX peut être déplacée vers et fonctionne sur toute plate-forme de gestionnaire de cellule. Une licence de Gestionnaire de cellule pour Windows ou Linux ne peut être déplacée vers et ne fonctionne pas pour une plate-forme de gestionnaire de cellule HP-UX.
>
> Toutes les autres licences peuvent être déplacées vers une plate-forme de gestionnaire de cellule sans restrictions. Le type de plate-forme de gestionnaire de cellule n'implique aucune restriction sur la licence. Par exemple, une licence de lecteur Windows peut être installée sur un gestionnaire de cellule HP-UX, cependant elle ne peut être utilisée pour un lecteur connecté à un système UNIX.

Pour déplacer les licences d'une instance de Gestionnaire de cellule à une autre :

1. Remplissez le *Formulaire de déplacement de licence* pour chaque nouveau Gestionnaire de cellule et envoyez-le au *Centre de délivrance de mot de passe.* Pour déplacer des licences pour les produits qui ne peuvent plus être achetés, vous devez utiliser les *Formulaires de déplacement de licence* délivrés avec la précédente version du produit. Voir Data Protector formulaires de licence, Page 307.

   Sur le formulaire, vous devez spécifier le nombre de licences que vous souhaitez déplacer depuis le Gestionnaire de cellule existant.

   En variante, rendez-vous sur le site web du centre de délivrance de mot de passe (https://software.microfocus.com/fr-fr/legal/software-licensing) et initiez le déplacement de licence en ligne.
2. Supprimez le fichier suivant :

   Systèmes Windows :

données_programme_Data_Protector\config\server\cell\lic.dat

Systèmes UNIX :

/etc/opt/omni/server/cell/lic.dat

3. Dès que vous avez rempli et envoyé le *Formulaire de déplacement de licence* au *Centre de délivrance de mot de passe (PDC)*, vous êtes légalement obligé d'effacer tous les mots de passe Data Protector de l'actuel Gestionnaire de cellule.
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 l'actuel Gestionnaire de cellule si les licences sont laissées sur l'actuel Gestionnaire de cellule. Ce nouveau mot de passe remplace l'actuel Gestionnaire de cellule.

> **REMARQUE :**
> Data Protector est également disponible dans le cadre de la suite ABR (Adaptive Backup and Recovery). La suite ABR combine une analyse de fichier non structurée et une hiérarchisation du stockage (Storage Optimizer) au moteur de protection principal (Data Protector) ainsi que des outils logiciels de rapport et d'analyse opérationnelle (Backup Navigator) pour offrir une approche innovante de la protection des données basée sur l'analyse et l'optimisation en temps réel.

Gestion centralisée des licences

Toutes les licences sont installées et conservées sur le système du Gestionnaire Manager-of-Managers (MoM). Les licences sont allouées à des cellules spécifiques bien qu'elles demeurent configurées sur le Manager MoM.

Pour plus d'informations sur la configuration des licences, reportez-vous à *Aide de Data Protector*.

> **REMARQUE :**
> Les licences de produit UNIX fonctionnent sur les plates-formes UNIX, Windows, et Novell NetWare, fournissant la fonctionnalité quelle que soit la plate-forme, tandis que les licences de produit Windows fonctionnent uniquement sur les plates-formes Windows, Novell NetWare et Linux.
>
> Une licence de Gestionnaire de cellule pour HP-UX peut être déplacée vers et fonctionne sur toute plate-forme de gestionnaire de cellule. Une licence de Gestionnaire de cellule pour Windows ou Linux ne peut être déplacée vers et ne fonctionne pas pour une plate-forme de gestionnaire de cellule HP-UX.
>
> Toutes les autres licences peuvent être déplacées vers une plate-forme de gestionnaire de cellule sans restrictions. Le type de plate-forme de gestionnaire de cellule n'implique aucune restriction sur la licence. Par exemple, une licence de lecteur Windows peut être installée sur un gestionnaire de cellule HP-UX, cependant elle ne peut être utilisée pour un lecteur connecté à un système UNIX.

La fonctionnalité MoM vous permet de déplacer (réassigner) des licences parmi les cellules MoM. Pour plus d'informations, reportez-vous à l'index *Aide de Data Protector* : "Environnement MoM".

Si vous installez une nouvelle licence Data Protector, assurez-vous de cocher la fonctionnalité MoM avant de demander une licence. Si vous décidez d'utiliser la gestion de licence centralisée ultérieurement, vous devrez alors recommencer la procédure de déplacement des licences.

Dans le cadre de la licence 100TB, vous recevrez une seule clé de licence. Il est impossible de recevoir de multiples clés pour l'attribution de licences Webware ou Micro Focus. Pour utiliser cette clé de licence unique, vous devez utiliser la gestion centralisée des licences dans l'environnement MoM. L'achat supplémentaire de 1TB LTU n'est pas requis, au lieu de cela 1TB LTU est attribué à chaque Gestionnaire de cellule même si cela nécessite 100GB.

> **REMARQUE :**
> La fonctionnalité MoM permet la gestion des licences centralisée. Ceci signifie que vous pouvez installer toutes les licences sur le Gestionnaire MoM puis les distribuer aux Gestionnaire de cellule qui appartiennent à la cellule MoM. Vous pouvez ultérieurement déplacer (redistribuer) les licences parmi les cellules MoM. Pour plus d'informations, reportez-vous à l'index *Aide de Data Protector* : "Environnement MoM".

Génération de rapports de licence

Les licences Data Protector sont vérifiées et s'il en manque, sont signalées au cours de différentes opérations de Data Protector, par exemple :

- Intégrées dans le mécanisme de vérification et de maintenance de Data Protector, les licences sont vérifiées et, s'il en manque, signalées dans le Journal des événements de Data Protector. Le journal d'événements de Data Protector est situé sur Gestionnaire de cellule dans *données_programme_Data_Protector*\log\server\Ob2EventLog.txt (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, reportez-vous à l'index *Aide de Data Protector* : "Journal des événements, Data Protector".
- Lorsque l'interface utilisateur de Data Protector est lancée, si des licences manquantes sont signalées dans le Journal des événements de Data Protector, une notification du Journal des événements est affichée. Pour plus de détails sur le Journal des événements de Data Protector, reportez-vous à l'index : "Jour*Aide de Data Protecto*nal des événements, Data Protector".
- Lorsqu'une session de Data Protector est démarrée, les licences sont vérifiées et, en cas d'absence, signalées.

Production d'un rapport de licences à la demande

Pour générer un rapport sur les licences de la cellule, exécutez :

```
omnicc -check_licenses [-detail]
```

Si l'option `-detail` est spécifiée, un rapport détaillé est généré. Pour chaque licence de la cellule, le vérificateur de licences renvoie les informations suivantes : nom de la licence, licences installées, licences utilisées, le total de To de données sous protection et les licences supplémentaires (capacité) requises.

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, serveur de licences et le total de To de données sous protection.

Notez que, pour les licences d'utilisation de l'extension de lecteur, le vérificateur de licences renvoie également 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.

Veuillez noter que la commande n'indique pas les dates d'expiration des licences. Selon l'environnement et le nombre de licences installées, la génération du rapport peut demander un certain temps. Pour obtenir les informations sur les dates d'expiration des licences, exécutez :

```
omnicc -password_info
```

> **IMPORTANT :**
> Dans un environnement MoM avec CMMDB configuré, en produisant un rapport de licence pour les éléments qui sont sujet aux bibliothèques et aux lecteurs, la commande `omnicc` doit être exécutée sur Gestionnaire de cellule avec CMMDB installé.
>
> Pour plus d'informations, reportez-vous à la page `omnicc` du manuel ou au *Guide de référence de l'interface de ligne de commande Data Protector*.

Mots de passe Data Protector

Une fois que vous avez installé le produit Data Protector, vous pouvez commencer à l'utiliser pendant 60 jours. Après cette période, vous devez installer un mot de passe permanent sur le Gestionnaire de cellule pour activer le logiciel. Vous pouvez charger le logiciel sur le Data Protector Gestionnaire de cellule, mais vous ne pouvez pas effectuer de tâches de configuration sans un mot de passe permanent, car les licences requises pour la fonctionnalité Data Protector particulière nécessitent des mots de passe.

La licence de Data Protector nécessite un des mots de passe suivants :

- Mot de passe Instant-On

  Un mot de passe Instant-On est intégré dans le produit à la première installation. Vous pouvez utiliser le logiciel pendant 60 jours après l'avoir installé sur tout système pris en charge par Data Protector. Au cours de cette période vous devez demander votre mot de passe permanent au *Centre de délivrance de mot de passe (PDC)* puis l'installer.

  Pour une installation existante de Data Protector, après la mise à jour vers 10.00 Data Protector ou ultérieur, votre installation est lancée avec un mot de passe Instant-On pendant 60 jours. Au cours de cette période, vous devez demander vos nouveaux mots de passe permanents au Centre de livraison de mot de passe comme spécifié dans votre accord d'assistance active. Les anciennes licences qui ne sont pas couvertes dans l'accord d'assistance ne peuvent être mises à jour.
- Mots de passe permanents

  Le produit Data Protector est distribué avec une licence *de Certificat* qui vous donne le droit d'obtenir un mot de passe permanent. Le mot de passe permanent vous permet de configurer une cellule Data Protector en relation avec votre stratégie de sauvegarde, dans la mesure où vous avez acheté les licences nécessaires. Avant de demander un mot de passe permanent, vous devez déterminer le système Gestionnaire de cellule et comprendre les exigences de configuration de votre cellule.
- Mot de passe d'urgence

  Les mots de passe d'urgence ou de repli sont disponibles au cas où les mots de passe actuellement installés ne correspondent pas avec la configuration système actuelle en raison d'une urgence. Ils permettront le fonctionnement sur tout système pour une durée de 120 jours.

Les mots de passe d'urgence sont produits par l'organisation d'assistance. Ils doivent être demandés par et sont produits uniquement pour le votre représentant assistance clientèle. Référez-vous à votre contact d'assistance ou consultez le site de licence à : https://software.microfocus.com/fr-fr/legal/software-licensing.

La finalité d'un mot de passe d'urgence est de permettre le fonctionnement d'une opération de sauvegarde tandis que la configuration système est reconstruite ou jusqu'à que vous effectuiez une nouvelle installation permanente. Dans le cas où vous déplacez les licences, vous devez remplir le Formulaire de déplacement de licence et l'envoyer au *Centre de délivrance de mot de passe (PDC)* ou rendez-vous sur la page web https://software.microfocus.com/fr-fr/legal/software-licensing où les mots de passe peuvent être générés, et ainsi de suite.

Pour les instructions sur la façon d'obtenir et d'installer un mot de passe, voir Obtention et installation des mots de passe, bas.

Obtention et installation des mots de passe

Obtention

Voici les procédures pour obtenir des mots de passe permanents :

1. Rassemble les informations nécessaires dans le *Formulaire de demande* de mot de passe permanent. Reportez-vous à Data Protector formulaires de licence, Page 307 pour trouver l'emplacement des formulaires et obtenir les instructions sur la manière de les remplir.
2. Reportez-vous à Data Protector Structure et licences de produit, Page 308 pour plus d'informations à propos de la structure de produit. Le *Centre de délivrance de mot de passe* vous enverra votre mot de passe permanent en utilisant le même moyen que celui que vous avez utilisé lorsque vous avez envoyé votre demande. Par exemple, si vous envoyez une requête par e-mail alors vous recevrez votre mot de passe permanent par e-mail.
3. Effectuez l'une des actions suivantes :
   - Rendez-vous sur le site en ligne du *Centre de délivrance de mot de passe* à l'adresse https://software.microfocus.com/fr-fr/legal/software-licensing.
   - Remplissez le *Formulaire de demande de mot de passe permanent* et envoyez-le au *Centre de délivrance de mot de passe* en utilisant un des éléments suivants (reportez-vous au Certificat envoyé avec le produit pour les numéros de fax, de téléphone, adresses e-mail et heures d'ouverture) :
     - Faxer un formulaire au *Centre de délivrance de mot de passe*
     - Envoyer un e-mail au *Centre de délivrance de mot de passe*

       Vous pouvez utiliser la version électronique des formulaires de licence qui sont inclus dans les fichiers suivants sur le Gestionnaire de cellule et le support d'installation :

       Sur Windows Gestionnaire de cellule: *répertoire_Data_Protector*`\Docs\license_forms.txt`

       Sur UNIX Gestionnaire de cellule: `/opt/omni/doc/C/license_forms_UNIX`

       pour “copier” et “coller” votre message au *Centre de délivrance de mot de passe (PDC)*.

       Vous recevrez votre mot de passe permanent dans les 24 heures suivant l'envoi de votre *Formulaire de demande de mot de passe permanent.*

Cette section décrit la procédure pour installer un mot de passe permanent que le *Centre de délivrance de mot de passe (PDC)* vous a envoyé.

Conditions préalables

Vous devez avoir reçu le mot de passe permanent envoyé par le *Centre de délivrance de mot de passe* et l'interface utilisateur Data Protector doit être installée sur le Gestionnaire de cellule. Les mots de passe sont installés sur le Gestionnaire de cellule et sont valides pour toute la cellule.

Utilisation de l'interface utilisateur graphique

Pour installer le mot de passe permanent en utilisant l'interface graphique utilisateur de Data Protector, procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, faites un clic droit sur **Data Protector Cellule** puis cliquez sur **Ajouter licence**.
3. Indiquez ou copiez le mot de passe exactement tel qu'il figure sur le *Certificat de mot de passe*.

   Un mot de passe se compose de 4 groupes de caractères de longueur variable, 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 :

   ```
   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR
   KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK
   ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX
   ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "Product; Cell Manager for UNIX"
   ```

   Une fois le mot de passe indiqué, vérifiez les points suivants :

   - 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 en fin du mot de passe, ni de caractères en trop.
   - Vérifiez que vous n'avez pas confondu les caractères "1" (chiffre un) et "l" (lettre l).
   - Vérifiez que vous n'avez pas confondu les caractères "O" (lettre majuscule) et "0" (chiffre).
   - Vérifiez que vous avez utilisé la bonne casse. La casse du mot de passe est prise en compte.

   Cliquez sur **OK**.

Le mot de passe est écrit dans le fichier suivant sur le Gestionnaire de cellule :

Systèmes Windows : *données_programme_Data_Protector*`\Config\server\Cell\lic.dat`

Systèmes UNIX : `/etc/opt/omni/server/cell/lic.dat`

Utilisation de l'interface de ligne de commande

Pour installer le mot de passe permanent en utilisant le CLI de Data Protector, procédez comme suit :

1. Identifiez-vous sur Gestionnaire de cellule.
2. Exécuter la commande suivante :

   `omnicc -install_license` *`password`*

   La chaîne *`password`* doit être saisie exactement telle qu'elle apparaît sur le *Certificat de mot de passe*. Il doit être formaté comme une ligne seule et ne doit pas contenir de retour à la ligne

intégré. Le mot de passe doit être entre guillemets. Si le mot de passe inclut également une description entre guillemets, les guillemets dans cette description doivent être précédés de barres obliques inversées. Pour un exemple et plus d'informations, reportez-vous à la page man `omnicc` ou au *Guide de référence de l'interface de ligne de commande Data Protector*.

Vous pouvez également ajouter le mot de passe au fichier suivant sur le Gestionnaire de cellule:

Systèmes Windows : *`données_programme_Data_Protector`*`\config\server\cell\lic.dat`

Systèmes UNIX : `/etc/opt/omni/server/cell/lic.dat`

Si le fichier n'existe pas, créez-le avec un éditeur, tel que vi ou Notepad. Pour un exemple de mot de passe, voirIndiquez ou copiez le mot de passe exactement tel qu'il figure sur le Certificat de mot de passe., Page 317 dans la procédure pour l'interface graphique utilisateur.

Vérification du mot de passe

Utilisation de l'interface utilisateur graphique

Pour vérifier si 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 **Licences**.
2. Cliquez sur l'onglet **Licences**. Toutes les licences installées sont affichées. Cliquez sur l'onglet **Infos mots de passe** pour voir les détails sur les mots de passe valides installés. Les mots de passe invalides seront marqués comme expirés ou supprimés.

   Toute la fenêtre pop-up ainsi que les colonnes individuelles sont redimensionnables.

Utilisation de l'interface de ligne de commande

Pour vérifier si le mot de passe pour la licence que vous avez installée est correct, utilisez la commande suivante :

```
omnicc -password_info
```

Cette commande affiche les licences installées. Si le mot de passe saisi est incorrect, il est listé avec la remarque `Password could not be decoded.`

Trouver le nombre de licences installées

Utilisation de l'interface utilisateur graphique

Une fois que vous avez installé un mot de passe permanent, vous pouvez vérifier le nombre de licences installées sur le Gestionnaire de cellule:

1. Démarrez Data Protector Manager.
2. Dans la barre du menu, cliquez sur **Aide**, puis **Licences...**. La fenêtre A propos de Manager s'ouvrira, affichant les licences installées.

Utilisation de l'interface de ligne de commande

Si vous utilisez la ligne de commande, procédez comme suit :

1. Identifiez-vous sur Gestionnaire de cellule.
2. Exécuter la commande suivante :

   ```
   omnicc -query
   ```

Un tableau listant les licences actuellement installées s'affichera.

Déplacer les licences vers un autre système Gestionnaire de cellule

Vous devez contacter le *Centre de délivrance de mot de passe* dans tous les cas suivants :

- Si vous souhaitez déplacer le Gestionnaire de cellule vers un autre système.
- Si vous prévoyez de déplacer une licence, installée sur un Gestionnaire de cellule qui n'est pas utilisé actuellement dans la cellule, vers une autre cellule Data Protector.

> **REMARQUE :**
> Les licences de produit UNIX fonctionnent sur les plates-formes UNIX, Windows, et Novell NetWare, fournissant la fonctionnalité quelle que soit la plate-forme, tandis que les licences de produit Windows fonctionnent uniquement sur les plates-formes Windows, Novell NetWare et Linux.
>
> Une licence de Gestionnaire de cellule pour HP-UX peut être déplacée vers et fonctionne sur toute plate-forme de gestionnaire de cellule. Une licence de Gestionnaire de cellule pour Windows ou Linux ne peut être déplacée vers et ne fonctionne pas pour une plate-forme de gestionnaire de cellule HP-UX.
>
> Toutes les autres licences peuvent être déplacées vers une plate-forme de gestionnaire de cellule sans restrictions. Le type de plate-forme de gestionnaire de cellule n'implique aucune restriction sur la licence. Par exemple, une licence de lecteur Windows peut être installée sur un gestionnaire de cellule HP-UX, cependant elle ne peut être utilisée pour un lecteur connecté à un système UNIX.

Pour déplacer les licences d'un Gestionnaire de cellule à une autre

1. Remplissez le *Formulaire de déplacement de licence* pour chaque nouveau Gestionnaire de cellule et envoyez-le au *Centre de délivrance de mot de passe.* Pour déplacer des licences pour les produits qui ne peuvent plus être achetés, vous devez utiliser les *Formulaires de déplacement de licence* délivrés avec la précédente version du produit. Voir Data Protector formulaires de licence, Page 307.

   Sur le formulaire, vous devez spécifier le nombre de licences que vous souhaitez déplacer depuis le Gestionnaire de cellule existant.

   En variante, rendez-vous sur le site web du centre de délivrance de mot de passe (https://software.microfocus.com/fr-fr/legal/software-licensing) et initiez le déplacement de licence en ligne.
2. Supprimez le fichier suivant :

   Systèmes Windows :

   données_programme_Data_Protector\config\server\cell\lic.dat

   Systèmes UNIX :

```
/etc/opt/omni/server/cell/lic.dat
```

3. Dès que vous avez rempli et envoyé le *Formulaire de déplacement de licence* au *Centre de délivrance de mot de passe (PDC)*, vous êtes légalement obligé d'effacer tous les mots de passe Data Protector de l'actuel Gestionnaire de cellule.
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 l'actuel Gestionnaire de cellule si les licences sont laissées sur l'actuel Gestionnaire de cellule. Ce nouveau mot de passe remplace l'actuel Gestionnaire de cellule.

Gestion centralisée des licences

Data Protector permet de configurer la gestion centralisée des licences pour l'ensemble d'un environnement d'entreprise constitué de plusieurs cellules, ce qui simplifie la gestion de licence. Toutes les licences sont installées et conservées sur le système du Gestionnaire Manager-of-Managers (MoM). Les licences sont allouées à des cellules spécifiques bien qu'elles demeurent configurées sur le Manager MoM.

Pour plus d'informations sur la configuration des licences, reportez-vous à *Aide de Data Protector*.

> **REMARQUE :**
> Les licences de produit UNIX fonctionnent sur les plates-formes UNIX, Windows, et Novell NetWare, fournissant la fonctionnalité quelle que soit la plate-forme, tandis que les licences de produit Windows fonctionnent uniquement sur les plates-formes Windows, Novell NetWare et Linux.
>
> Une licence de Gestionnaire de cellule pour HP-UX peut être déplacée vers et fonctionne sur toute plate-forme de gestionnaire de cellule. Une licence de Gestionnaire de cellule pour Windows ou Linux ne peut être déplacée vers et ne fonctionne pas pour une plate-forme de gestionnaire de cellule HP-UX.
>
> Toutes les autres licences peuvent être déplacées vers une plate-forme de gestionnaire de cellule sans restrictions. Le type de plate-forme de gestionnaire de cellule n'implique aucune restriction sur la licence. Par exemple, une licence de lecteur Windows peut être installée sur un gestionnaire de cellule HP-UX, cependant elle ne peut être utilisée pour un lecteur connecté à un système UNIX.

La fonctionnalité MoM vous permet de déplacer (réassigner) des licences parmi les cellules MoM. Pour plus d'informations, reportez-vous à l'index *Aide de Data Protector* : “Environnement MoM”.

Si vous installez une nouvelle licence Data Protector, assurez-vous de cocher la fonctionnalité MoM avant de demander une licence. Si vous décidez d'utiliser la gestion de licence centralisée ultérieurement, vous devrez alors recommencer la procédure de déplacement des licences.

> **REMARQUE :**
> La fonctionnalité MoM permet la gestion des licences centralisée. Ceci signifie que vous pouvez installer toutes les licences sur le Gestionnaire MoM puis les distribuer aux Gestionnaire de cellule qui appartiennent à la cellule MoM. Vous pouvez ultérieurement déplacer (redistribuer) les licences parmi les cellules MoM. Pour plus d'informations, reportez-vous à l'index *Aide de Data Protector* : “Environnement MoM”.

Migration de licence vers Data Protector 10.00

Data Protector 8.1 et les clients suivants sur le contrat d'assistance recevront Data Protector 10.00 gratuitement incluant de nouvelles clés de licence pour toutes les licences sur le contrat d'assistance.

Data Protector 10.00 n'affiche pas les licences qui sont expirées ou inutilisées pour la même version de produit.

Vous pouvez vous rendre sur le portail MyUpdates sur le Software Support Online (SSO) https://softwaresupport.softwaregrp.com/.

Vous aurez accès au téléchargement du logiciel et des clés de licence que vous êtes en droit d'obtenir en accord avec votre contrat d'assistance actif (SAID).

Vous pouvez voir tous les logiciels associés au SAID, cochez la case devant le Data Protector 10.00 ou versions ultérieures et cliquez sur **Obtenir les mises à jour**.

Trois onglets sont proposés :

- **Obtenir le logiciel** : Pour télécharger le logiciel.
- **Obtenir les licences** : Pour obtenir des licences pour les LTU schéématisés vers Data Protector 9.00 ou versions ultérieures.
- **Obtenir des documents :** Pour télécharger la documentation du produit.

Lorsque vous cliquez sur le lien **Obtenir la licence**, vous êtes redirigé vers la commande de mise à jour de the Software Licensing Portal (https://software.microfocus.com/fr-fr/legal/software-licensing) où vous pouvez obtenir les clés de licence pour les LTU et les quantités qui sont sur Service Agreement Identifier (SAID).

Data Protector formulaires de licence

Cette section présente les Data Protector formulaires de licence. Remplissez-les pour commander des mots de passe permanents en utilisant un des moyens suivants :

- Commandez des mots de passe permanents en utilisant le site du *Centre de délivrance de mot de passe* en ligne à l'adresse https://software.microfocus.com/fr-fr/legal/software-licensing.
- Imprimez la version électronique des formulaires de licence qui sont inclus dans les fichiers suivants sur le système Gestionnaire de cellule et le support d'installation :

  Systèmes HP-UX et Linux : `/opt/omni/doc/C/license_forms_UNIX`

  Package d'installation Windows : *`DriveLetter`*`:Docs\license_forms.txt`

  ou utilisez les fichiers électroniques pour “copier” et “coller” votre message au *Centre de délivrance de mot de passe (PDC)*.

> **IMPORTANT :**
> Assurez-vous de saisir clairement les informations et que vous n'oubliez pas les champs obligatoires.

Les champs généraux dans les formulaires de licence que vous devez remplir sont brièvement décrits en dessous :

Données personnelles	Ce champ contient les informations client, comprenant la personne à qui le nouveau mot de passe doit être délivré.
Données de licence	Fournissez les informations de licence à propos de votre cellule Data Protector.
Gestionnaire de cellule actuel	Fournissez les informations nécessaires concernant l'actuel Gestionnaire de cellule.
Nouveau Gestionnaire de cellule	Fournissez les informations nécessaires concernant votre nouveau Gestionnaire de cellule.
Numéro de commande	Saisissez le *Numéro de commande* imprimé sur le *Certificat.* Le *Numéro de commande* est nécessaire pour vérifier que vous êtes en droit de demander un mot de passe permanent.
Adresse IP	Ce champ définit le système pour lequel le *Centre de délivrance de mot de passe* générera les mots de passe. Au cas où vous voulez utiliser la gestion de licence centralisée (environnement MoM uniquement) alors ce système doit être le système de Gestionnaire MoM. Si le Gestionnaire de cellule dispose de plusieurs cartes LAN, vous pouvez saisir n'importe laquelle des adresses IP. Micro Focus recommande que vous saisissiez la première. Si vous avez Data Protector dans un environnement Serviceguard ou Microsoft Cluster, saisissez l'adresse IP de votre serveur virtuel. Pour plus d'informations sur les clusters, reportez-vous au *Aide de Data Protector*.
Les numéros de fax du *Centre de délivrance de mot de passe*	Pour des informations de contact, reportez-vous au *Certificat* distribué avec votre produit.
Type de licence produit	Dans les champs près des *Numéros de produit*, saisissez la quantité de licences que vous voulez installer sur ce Gestionnaire de cellule. La quantité peut être la totalité ou bien un sous-ensemble des licences achetées avec le *Numéro de commande*.

Data Protector Structure et licences de produit

Considérations relatives aux mots de passe

Considérez les éléments suivants pour aider à déterminer le bon nombre de mots de passe.

- Les mots de passe Instant-On sont intégrés. Ils sont disponibles pour chaque nouvelle installation et chaque installation existante de Data Protector mise à niveau vers la version Data Protector10.00 ou ultérieure pour 60 jours sans autre exigence d'installation de licence de mot de passe supplémentaire, et ils vous offrent la fonctionnalité complète du produit à des fins d'évaluation.

Après 60 jours, les mots de passe instant-On expirent et le produit cesse de fonctionner, à moins qu'une clé de licence permanente ait été installée.

> **IMPORTANT :**
> La période d'installation pour le produit complet se termine dès que la clé de licence normale est installée. Dès qu'au moins une clé de licence est installée, seule la fonctionnalité peut être utilisée, pour laquelle les clés de licence ont été installées.

- Les licences permanentes peuvent être déplacées vers un Gestionnaire de cellule différent. Cependant, vous devez utiliser le Formulaire de déplacement de licence et l'envoyer au *Password Delivery Center (PDC)* de.
- Les mots de passe sont installés sur le Gestionnaire de cellule et valides pour toute la cellule.
- La licence centralisée est fournie dans la fonctionnalité de Manager-of-Managers (MoM). Vous pouvez installer toutes les licences sur le système MoM si vous achetez des licences multiples pour plusieurs cellules.
- Vous avez besoin d'une licence Gestionnaire de cellule pour chaque cellule.
- Les clés de licence ou mots de passe sont régulièrement vérifiés par le logiciel lorsque vous effectuez une mission de configuration de Data Protector ou démarrez une session de sauvegarde.
- Les mots de passe Instant-On peuvent être utilisés sur tout système, tandis que les mots de passe d'évaluation et permanents ne peuvent être utilisés que pour le système Gestionnaire de cellule pour lequel vous avez demandé les licences.

> **REMARQUE :**
> Pour modifier l'adresse IP de Gestionnaire de cellule, pour déplacer le Gestionnaire de cellule vers un autre système, ou pour déplacer des licences d'une cellule vers une autre (où la fonctionnalité MoM n'est pas utilisée), vous devez contacter le *Password Delivery Center (PDC)* afin de mettre à jour les licences. Pour des informations sur la manière de contacter le Password Delivery Center de, reportez-vous à *Obtention et installation de mots passe permanents*.

Mots de passe Data Protector

Une fois que vous avez installé le produit Data Protector, vous pouvez commencer à l'utiliser pendant 60 jours. Après cette période, vous devez installer un mot de passe permanent sur le Gestionnaire de cellule pour activer le logiciel. Vous pouvez charger le logiciel sur le Data Protector Gestionnaire de cellule, mais vous ne pouvez pas effectuer de tâches de configuration sans un mot de passe permanent, car les licences requises pour la fonctionnalité Data Protector particulière nécessitent des mots de passe.

La licence de Data Protector nécessite un des mots de passe suivants :

- Mot de passe Instant-On

  Un mot de passe Instant-On est intégré dans le produit à la première installation. Vous pouvez utiliser le logiciel pendant 60 jours après l'avoir installé sur tout système pris en charge par Data Protector. Au cours de cette période vous devez demander votre mot de passe permanent au *Centre de délivrance de mot de passe (PDC)* puis l'installer.

  Pour une installation existante de Data Protector, après la mise à jour vers 10.00 Data Protector ou ultérieur, votre installation est lancée avec un mot de passe Instant-On pendant 60 jours. Au cours

de cette période, vous devez demander vos nouveaux mots de passe permanents au Centre de livraison de mot de passe comme spécifié dans votre accord d'assistance active. Les anciennes licences qui ne sont pas couvertes dans l'accord d'assistance ne peuvent être mises à jour.

- Mots de passe permanents

  Le produit Data Protector est distribué avec une licence *de Certificat* qui vous donne le droit d'obtenir un mot de passe permanent. Le mot de passe permanent vous permet de configurer une cellule Data Protector en relation avec votre stratégie de sauvegarde, dans la mesure où vous avez acheté les licences nécessaires. Avant de demander un mot de passe permanent, vous devez déterminer le système Gestionnaire de cellule et comprendre les exigences de configuration de votre cellule.

- Mot de passe d'urgence

  Les mots de passe d'urgence ou de repli sont disponibles au cas où les mots de passe actuellement installés ne correspondent pas avec la configuration système actuelle en raison d'une urgence. Ils permettront le fonctionnement sur tout système pour une durée de 120 jours.

  Les mots de passe d'urgence sont produits par l'organisation d'assistance. Ils doivent être demandés par et sont produits uniquement pour le votre représentant assistance clientèle. Référez-vous à votre contact d'assistance ou consultez le site de licence à : https://software.microfocus.com/fr-fr/legal/software-licensing.

  La finalité d'un mot de passe d'urgence est de permettre le fonctionnement d'une opération de sauvegarde tandis que la configuration système est reconstruite ou jusqu'à que vous effectuiez une nouvelle installation permanente. Dans le cas où vous déplacez les licences, vous devez remplir le Formulaire de déplacement de licence et l'envoyer au *Centre de délivrance de mot de passe (PDC)* ou rendez-vous sur la page web https://software.microfocus.com/fr-fr/legal/software-licensing où les mots de passe peuvent être générés, et ainsi de suite.

Pour les instructions sur la façon d'obtenir et d'installer un mot de passe, voir Obtention et installation des mots de passe, bas.

Obtention et installation des mots de passe

Obtention

Voici les procédures pour obtenir des mots de passe permanents :

1. Rassemble les informations nécessaires dans le *Formulaire de demande* de mot de passe permanent. Reportez-vous à Data Protector formulaires de licence, Page 307 pour trouver l'emplacement des formulaires et obtenir les instructions sur la manière de les remplir.
2. Reportez-vous à Data Protector Structure et licences de produit, Page 308 pour plus d'informations à propos de la structure de produit. Le *Centre de délivrance de mot de passe* vous enverra votre mot de passe permanent en utilisant le même moyen que celui que vous avez utilisé lorsque vous avez envoyé votre demande. Par exemple, si vous envoyez une requête par e-mail alors vous recevrez votre mot de passe permanent par e-mail.
3. Effectuez l'une des actions suivantes :
   - Rendez-vous sur le site en ligne du *Centre de délivrance de mot de passe* à l'adresse https://software.microfocus.com/fr-fr/legal/software-licensing.
   - Remplissez le *Formulaire de demande de mot de passe permanent* et envoyez-le au *Centre de délivrance de mot de passe* en utilisant un des éléments suivants (reportez-vous au Certificat

envoyé avec le produit pour les numéros de fax, de téléphone, adresses e-mail et heures d'ouverture) :

- Faxer un formulaire au *Centre de délivrance de mot de passe*
- Envoyer un e-mail au *Centre de délivrance de mot de passe*

  Vous pouvez utiliser la version électronique des formulaires de licence qui sont inclus dans les fichiers suivants sur le Gestionnaire de cellule et le support d'installation :

  Sur Windows Gestionnaire de cellule: *répertoire_Data_Protector*\Docs\license_forms.txt

  Sur UNIX Gestionnaire de cellule: /opt/omni/doc/C/license_forms_UNIX

  pour “copier” et “coller” votre message au *Centre de délivrance de mot de passe (PDC)*.

  Vous recevrez votre mot de passe permanent dans les 24 heures suivant l'envoi de votre *Formulaire de demande de mot de passe permanent.*

Cette section décrit la procédure pour installer un mot de passe permanent que le *Centre de délivrance de mot de passe (PDC)* vous a envoyé.

Conditions préalables

Vous devez avoir reçu le mot de passe permanent envoyé par le *Centre de délivrance de mot de passe* et l'interface utilisateur Data Protector doit être installée sur le Gestionnaire de cellule. Les mots de passe sont installés sur le Gestionnaire de cellule et sont valides pour toute la cellule.

Utilisation de l'interface utilisateur graphique

Pour installer le mot de passe permanent en utilisant l'interface graphique utilisateur de Data Protector, procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, faites un clic droit sur **Data Protector Cellule** puis cliquez sur **Ajouter licence**.
3. Indiquez ou copiez le mot de passe exactement tel qu'il figure sur le *Certificat de mot de passe*.

   Un mot de passe se compose de 4 groupes de caractères de longueur variable, 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 :

   ```
   QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR
   KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK
   ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX
   ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "Product; Cell Manager for UNIX"
   ```

   Une fois le mot de passe indiqué, vérifiez les points suivants :

   - 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 en fin du mot de passe, ni de caractères en trop.
   - Vérifiez que vous n'avez pas confondu les caractères "1" (chiffre un) et "l" (lettre l).

- Vérifiez que vous n'avez pas confondu les caractères "O" (lettre majuscule) et "0" (chiffre).
- Vérifiez que vous avez utilisé la bonne casse. La casse du mot de passe est prise en compte.

Cliquez sur **OK**.

Le mot de passe est écrit dans le fichier suivant sur le Gestionnaire de cellule :

Systèmes Windows : *données_programme_Data_Protector*\Config\server\Cell\lic.dat

Systèmes UNIX : /etc/opt/omni/server/cell/lic.dat

Utilisation de l'interface de ligne de commande

Pour installer le mot de passe permanent en utilisant le CLI de Data Protector, procédez comme suit :

1. Identifiez-vous sur Gestionnaire de cellule.
2. Exécuter la commande suivante :

   omnicc -install_license *password*

   La chaîne *password* doit être saisie exactement telle qu'elle apparaît sur le *Certificat de mot de passe*. Il doit être formaté comme une ligne seule et ne doit pas contenir de retour à la ligne intégré. Le mot de passe doit être entre guillemets. Si le mot de passe inclut également une description entre guillemets, les guillemets dans cette description doivent être précédés de barres obliques inversées. Pour un exemple et plus d'informations, reportez-vous à la page man omnicc ou au *Guide de référence de l'interface de ligne de commande Data Protector*.

Vous pouvez également ajouter le mot de passe au fichier suivant sur le Gestionnaire de cellule:

Systèmes Windows : *données_programme_Data_Protector*\config\server\cell\lic.dat

Systèmes UNIX : /etc/opt/omni/server/cell/lic.dat

Si le fichier n'existe pas, créez-le avec un éditeur, tel que vi ou Notepad. Pour un exemple de mot de passe, voirIndiquez ou copiez le mot de passe exactement tel qu'il figure sur le Certificat de mot de passe., Page 317 dans la procédure pour l'interface graphique utilisateur.

Vérification du mot de passe

Utilisation de l'interface utilisateur graphique

Pour vérifier si 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 **Licences**.
2. Cliquez sur l'onglet **Licences**. Toutes les licences installées sont affichées. Cliquez sur l'onglet **Infos mots de passe** pour voir les détails sur les mots de passe valides installés. Les mots de passe invalides seront marqués comme expirés ou supprimés.

   Toute la fenêtre pop-up ainsi que les colonnes individuelles sont redimensionnables.

Utilisation de l'interface de ligne de commande

Pour vérifier si le mot de passe pour la licence que vous avez installée est correct, utilisez la commande suivante :

```
omnicc -password_info
```

Cette commande affiche les licences installées. Si le mot de passe saisi est incorrect, il est listé avec la remarque `Password could not be decoded.`

Trouver le nombre de licences installées

Utilisation de l'interface utilisateur graphique

Une fois que vous avez installé un mot de passe permanent, vous pouvez vérifier le nombre de licences installées sur le Gestionnaire de cellule:

1. Démarrez Data Protector Manager.
2. Dans la barre du menu, cliquez sur **Aide**, puis **Licences...**. La fenêtre A propos de Manager s'ouvrira, affichant les licences installées.

Utilisation de l'interface de ligne de commande

Si vous utilisez la ligne de commande, procédez comme suit :

1. Identifiez-vous sur Gestionnaire de cellule.
2. Exécuter la commande suivante :

   ```
   omnicc -query
   ```

Un tableau listant les licences actuellement installées s'affichera.

Déplacer les licences vers un autre système Gestionnaire de cellule

Vous devez contacter le *Centre de délivrance de mot de passe* dans tous les cas suivants :

- Si vous souhaitez déplacer le Gestionnaire de cellule vers un autre système.
- Si vous prévoyez de déplacer une licence, installée sur un Gestionnaire de cellule qui n'est pas utilisé actuellement dans la cellule, vers une autre cellule Data Protector.

> **REMARQUE :**
> Les licences de produit UNIX fonctionnent sur les plates-formes UNIX, Windows, et Novell NetWare, fournissant la fonctionnalité quelle que soit la plate-forme, tandis que les licences de produit Windows fonctionnent uniquement sur les plates-formes Windows, Novell NetWare et Linux.
>
> Une licence de Gestionnaire de cellule pour HP-UX peut être déplacée vers et fonctionne sur toute plate-forme de gestionnaire de cellule. Une licence de Gestionnaire de cellule pour Windows ou Linux ne peut être déplacée vers et ne fonctionne pas pour une plate-forme de gestionnaire de cellule HP-UX.
>
> Toutes les autres licences peuvent être déplacées vers une plate-forme de gestionnaire de cellule sans restrictions. Le type de plate-forme de gestionnaire de cellule n'implique aucune restriction sur la licence. Par exemple, une licence de lecteur Windows peut être installée sur un gestionnaire de cellule HP-UX, cependant elle ne peut être utilisée pour un lecteur connecté à un système UNIX.

Pour déplacer les licences d'un Gestionnaire de cellule à une autre

1. Remplissez le *Formulaire de déplacement de licence* pour chaque nouveau Gestionnaire de cellule et envoyez-le au *Centre de délivrance de mot de passe.* Pour déplacer des licences pour les produits qui ne peuvent plus être achetés, vous devez utiliser les *Formulaires de déplacement de licence* délivrés avec la précédente version du produit. Voir Data Protector formulaires de licence, Page 307.

   Sur le formulaire, vous devez spécifier le nombre de licences que vous souhaitez déplacer depuis le Gestionnaire de cellule existant.

   En variante, rendez-vous sur le site web du centre de délivrance de mot de passe (https://software.microfocus.com/fr-fr/legal/software-licensing) et initiez le déplacement de licence en ligne.
2. Supprimez le fichier suivant :

   Systèmes Windows :

   données_programme_Data_Protector\config\server\cell\lic.dat

   Systèmes UNIX :

   /etc/opt/omni/server/cell/lic.dat
3. Dès que vous avez rempli et envoyé le *Formulaire de déplacement de licence* au *Centre de délivrance de mot de passe (PDC)*, vous êtes légalement obligé d'effacer tous les mots de passe Data Protector de l'actuel Gestionnaire de cellule.
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 l'actuel Gestionnaire de cellule si les licences sont laissées sur l'actuel Gestionnaire de cellule. Ce nouveau mot de passe remplace l'actuel Gestionnaire de cellule.

Gestion centralisée des licences

Data Protector permet de configurer la gestion centralisée des licences pour l'ensemble d'un environnement d'entreprise constitué de plusieurs cellules, ce qui simplifie la gestion de licence. Toutes les licences sont installées et conservées sur le système du Gestionnaire Manager-of-Managers (MoM). Les licences sont allouées à des cellules spécifiques bien qu'elles demeurent configurées sur le Manager MoM.

Pour plus d'informations sur la configuration des licences, reportez-vous à *Aide de Data Protector*.

> **REMARQUE :**
> Les licences de produit UNIX fonctionnent sur les plates-formes UNIX, Windows, et Novell NetWare, fournissant la fonctionnalité quelle que soit la plate-forme, tandis que les licences de produit Windows fonctionnent uniquement sur les plates-formes Windows, Novell NetWare et Linux.
>
> Une licence de Gestionnaire de cellule pour HP-UX peut être déplacée vers et fonctionne sur toute plate-forme de gestionnaire de cellule. Une licence de Gestionnaire de cellule pour Windows ou Linux ne peut être déplacée vers et ne fonctionne pas pour une plate-forme de gestionnaire de cellule HP-UX.
>
> Toutes les autres licences peuvent être déplacées vers une plate-forme de gestionnaire de cellule sans restrictions. Le type de plate-forme de gestionnaire de cellule n'implique aucune

> restriction sur la licence. Par exemple, une licence de lecteur Windows peut être installée sur un gestionnaire de cellule HP-UX, cependant elle ne peut être utilisée pour un lecteur connecté à un système UNIX.

La fonctionnalité MoM vous permet de déplacer (réassigner) des licences parmi les cellules MoM. Pour plus d'informations, reportez-vous à l'index *Aide de Data Protector* : “Environnement MoM”.

Si vous installez une nouvelle licence Data Protector, assurez-vous de cocher la fonctionnalité MoM avant de demander une licence. Si vous décidez d'utiliser la gestion de licence centralisée ultérieurement, vous devrez alors recommencer la procédure de déplacement des licences.

> **REMARQUE :**
> La fonctionnalité MoM permet la gestion des licences centralisée. Ceci signifie que vous pouvez installer toutes les licences sur le Gestionnaire MoM puis les distribuer aux Gestionnaire de cellule qui appartiennent à la cellule MoM. Vous pouvez ultérieurement déplacer (redistribuer) les licences parmi les cellules MoM. Pour plus d'informations, reportez-vous à l'index *Aide de Data Protector* : “Environnement MoM”.

Mot de passe de licence

Une fois que vous avez installé le produit Data Protector, vous pouvez commencer à l'utiliser pendant 60 jours. Après cette période, vous devez installer un mot de passe permanent sur le Gestionnaire de cellule pour activer le logiciel. Vous pouvez charger le logiciel sur le Data ProtectorGestionnaire de cellule, mais vous ne pouvez pas effectuer de tâches de configuration sans un mot de passe permanent, car les licences requises pour la fonctionnalité Data Protector particulière nécessitent des mots de passe.

Considérations relatives aux mots de passe

Considérez les éléments suivants pour aider à déterminer le bon nombre de mots de passe :

- Les mots de passe Instant-On sont intégrés. Ils sont disponibles pour chaque nouvelle installation et chaque installation existante de Data Protector mise à jour vers la version Data Protector 9.00 ou ultérieure pendant 60 jours sans autre exigence d'installation de licence de mot de passe supplémentaire, et ils vous offrent la fonctionnalité complète du produit à des fins d'évaluation.

  Après 60 jours, les mots de passe instant-On expirent et le produit cesse de fonctionner, à moins qu'une clé de licence permanente ait été installée.

  La période d'installation pour le produit complet se termine dès que la clé de licence normale est installée. Dès qu'au moins une clé de licence est installée, seule la fonctionnalité peut être utilisée, pour laquelle les clés de licence ont été installées.
- Les licences permanentes peuvent être déplacées vers un Gestionnaire de cellule différent. Toutefois, vous devez utiliser le(s) formulaire(s) de déplacement de licence et le(s) envoyer au Centre de délivrance de mot de passe.
- Les mots de passe sont installés sur le Gestionnaire de cellule et valables pour toute la cellule.
- La licence centralisée est fournie dans la fonctionnalité de Manager-of-Managers (MoM). Vous pouvez installer toutes les licences sur le système MoM si vous achetez des licences multiples pour plusieurs cellules.

- Vous avez besoin d'une licence de Gestionnaire de cellule pour chaque cellule.
- Les clés de licence ou mots de passe sont régulièrement vérifiés par le logiciel lorsque vous effectuez une mission de configuration de Data Protector ou démarrez une session de sauvegarde.
- Les mots de passe Instant-On peuvent être utilisés sur tout système, tandis que les mots de passe d'évaluation et permanents ne peuvent être utilisés que pour le système du Gestionnaire de cellule pour lequel vous avez demandé les licences.

La licence de Data Protector nécessite un des mots de passe suivants :

- Mot de passe Instant-On

  Un mot de passe Instant-On est intégré dans le produit à la première installation. Vous pouvez utiliser le logiciel pendant 60 jours après l'avoir installé sur tout système pris en charge par Data Protector. Au cours de cette période vous devez demander votre mot de passe permanent au *Centre de délivrance de mot de passe (PDC)* puis l'installer.

  Pour une installation existante de Data Protector, apres la mise a jour vers ou ultérieur, Data Protector9.00votre installation est lancée avec un mot de passe Instant-On pendant 60 jours. Au cours de cette période, vous devez demander vos nouveaux mots de passe permanents au Centre de livraison de mot de passe comme spécifié dans votre accord d'assistance active. Les anciennes licences qui ne sont pas couvertes dans l'accord d'assistance ne peuvent être mises à jour.
- Mots de passe permanents

  Le produit Data Protector est distribué avec une licence *de Certificat* qui vous donne le droit d'obtenir un mot de passe permanent. Le mot de passe permanent vous permet de configurer une cellule Data Protector en relation avec votre stratégie de sauvegarde, dans la mesure où vous avez acheté les licences nécessaires. Avant de demander un mot de passe permanent, vous devez déterminer le système Gestionnaire de cellule et comprendre les exigences de configuration de votre cellule.
- Mot de passe d'urgence

  Les mots de passe d'urgence ou de repli sont disponibles au cas où les mots de passe actuellement installés ne correspondent pas avec la configuration système actuelle en raison d'une urgence. Ils permettront le fonctionnement sur tout système pour une durée de 120 jours.

  Les mots de passe d'urgence sont produits par l'organisation d'assistance. Ils doivent être demandés par et sont produits uniquement pour le personnel de. Référez-vous à votre contact d'assistance ou consultez le site de licence de à : https://software.microfocus.com/fr-fr/legal/software-licensing.

  La finalité d'un mot de passe d'urgence est de permettre le fonctionnement d'une opération de sauvegarde tandis que la configuration système est reconstruite ou jusqu'à que vous effectuiez une nouvelle installation permanente. Dans le cas où vous déplacez les licences, vous devez remplir le Formulaire de déplacement de licence et l'envoyer au *Centre de délivrance de mot de passe (PDC)* ou rendez-vous sur la page web https://software.microfocus.com/fr-fr/legal/software-licensing où les mots de passe peuvent être générés, et ainsi de suite.

Pour les instructions sur la façon d'obtenir et d'installer un mot de passe, voir Obtention de mots de passe permanents, bas.

Obtention de mots de passe permanents

Voici les procédures pour obtenir des mots de passe permanents :

1. Rassemble les informations nécessaires dans le *Formulaire de demande* de mot de passe permanent. Reportez-vous à Formulaires de licence Data Protector, Page suivante pour trouver l'emplacement des formulaires et obtenir les instructions sur la manière de les remplir.
2. Le *Centre de délivrance de mot de passe* vous enverra votre mot de passe permanent en utilisant le même moyen que celui que vous avez utilisé lorsque vous avez envoyé votre demande. Par exemple, si vous envoyez une requête par e-mail alors vous recevrez votre mot de passe permanent par e-mail.
3. Effectuez l'une des actions suivantes :
   - Rendez-vous sur le site en ligne du *Centre de délivrance de mot de passe* à l'adresse https://software.microfocus.com/fr-fr/legal/software-licensing.
   - Remplissez le *Formulaire de demande de mot de passe permanent* et envoyez-le au *Centre de délivrance de mot de passe* en utilisant un des éléments suivants (reportez-vous au Certificat envoyé avec le produit pour les numéros de fax, de téléphone, adresses e-mail et heures d'ouverture) :
     - Faxer un formulaire au *Centre de délivrance de mot de passe*
     - Envoyer un e-mail au *Centre de délivrance de mot de passe*

       Vous pouvez utiliser la version électronique des formulaires de licence qui sont inclus dans les fichiers suivants sur le Gestionnaire de cellule et le support d'installation :

       Sur Windows Gestionnaire de cellule :`répertoire_Data_Protector\Docs\license_forms.txt`

       Sur UNIX Gestionnaire de cellule :`/opt/omni/doc/C/license_forms_UNIX`

       Dans le package d'installation Windows :`Disk_Label:\Docs\license_forms.txt`

       pour “copier” et “coller” votre message au *Centre de délivrance de mot de passe (PDC)*.

       Vous recevrez votre mot de passe permanent dans les 24 heures suivant l'envoi de votre *Formulaire de demande de mot de passe permanent.*

Installation des mots de passe permanents

Cette section décrit la procédure pour installer un mot de passe permanent que le *Centre de délivrance de mot de passe (PDC)* vous a envoyé.

Conditions préalables :

Vous devez avoir reçu le mot de passe permanent envoyé par le *Centre de délivrance de mot de passe* et l'interface utilisateur Data Protector doit être installée sur le Gestionnaire de cellule. Les mots de passe sont installés sur le Gestionnaire de cellule et sont valides pour toute la cellule.

Utilisation de l'interface utilisateur graphique :

Pour installer le mot de passe permanent en utilisant l'interface graphique utilisateur de Data Protector, procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, faites un clic droit sur **Data Protector Cellule** puis cliquez sur **Ajouter licence**.
3. Indiquez ou copiez le mot de passe exactement tel qu'il figure sur le *Certificat de mot de passe*.

Un mot de passe se compose de 4 groupes de caractères de longueur variable, 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 :

```
QB9A AQEA H9PQ KHU2 UZD4 H8S5 Y9JL 2MPL B89H MZVU EUJV KCS9 KHU4 9AC2 CRYP DXMR
KLLK XVSS GHU6 D2RJ N6KJ 2KG8 PVRJ 37LX DJ2J EWMB A3PG 96QY E2AW WF8E NMXC LNCK
ZVWM 9AKS PU3U WCZ8 PSJ5 PQKM 5KCC FYDE 4MPM 9GUB C647 WEQX 4NMU BGN5 L8SM 23TX
ANTR VFPJ PSJL KTQW U8NK H4H4 TB4K L4XQ "Product; Cell Manager for UNIX"
```

Une fois le mot de passe indiqué, vérifiez les points suivants :

- 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 en fin du mot de passe, ni de caractères en trop.
- Vérifiez que vous n'avez pas confondu les caractères "1" (chiffre un) et "l" (lettre l).
- Vérifiez que vous n'avez pas confondu les caractères "O" (lettre majuscule) et "0" (chiffre).
- Vérifiez que vous avez utilisé la bonne casse. La casse du mot de passe est prise en compte.

Cliquez sur **OK**.

Le mot de passe est écrit dans le fichier suivant sur le Gestionnaire de cellule :

Systèmes Windows :*données_programme_Data_Protector*\Config\server\Cell\lic.dat

Systèmes UNIX :/etc/opt/omni/server/cell/lic.dat

Utilisation de l'interface de ligne de commande :

Pour installer le mot de passe permanent en utilisant le CLI de Data Protector, procédez comme suit :

1. Identifiez-vous sur Gestionnaire de cellule.
2. Exécuter la commande suivante :

   ```
   omnicc -install_license password
   ```

   La chaîne *password* doit être saisie exactement telle qu'elle apparaît sur le *Certificat de mot de passe*. Il doit être formaté comme une ligne seule et ne doit pas contenir de retour à la ligne intégré. Le mot de passe doit être entre guillemets. Si le mot de passe inclut également une description entre guillemets, les guillemets dans cette description doivent être précédés de barres obliques inversées. Pour un exemple et plus d'informations, reportez-vous à la page man `omnicc` ou au *Guide de référence de l'interface de ligne de commande Data Protector*.

Vous pouvez également ajouter le mot de passe au fichier suivant sur le Gestionnaire de cellule:

Systèmes Windows :*données_programme_Data_Protector*\config\server\cell\lic.dat

Systèmes UNIX :/etc/opt/omni/server/cell/lic.dat

Si le fichier n'existe pas, créez-le avec un éditeur, tel que `vi` ou `Notepad`. Pour un exemple de mot de passe, voir Indiquez ou copiez le mot de passe exactement tel qu'il figure sur le Certificat de mot de passe., Page précédente dans la procédure pour l'interface graphique utilisateur.

Formulaires de licence Data Protector

Cette section présente les Data Protector formulaires de licence. Remplissez-les pour commander des mots de passe permanents en utilisant un des moyens suivants :

- Commandez des mots de passe permanents en utilisant le site du *Centre de délivrance de mot de passe* en ligne à l'adresse https://software.microfocus.com/fr-fr/legal/software-licensing.
- Imprimez la version électronique des formulaires de licence qui sont inclus dans les fichiers suivants sur le système Gestionnaire de cellule et le support d'installation :

  Systèmes HP-UX et Linux :`/opt/omni/doc/C/license_forms_UNIX`

  Package d'installation Windows :`Docs\license_forms.txt`

  ou utilisez les fichiers électroniques pour “copier” et “coller” votre message au *Centre de délivrance de mot de passe (PDC)*.

> **IMPORTANT :**
> Assurez-vous de saisir clairement les informations et que vous n'oubliez pas les champs obligatoires.

Les champs généraux dans les formulaires de licence que vous devez remplir sont brièvement décrits en dessous :

Données personnelles	Ce champ contient les informations client, comprenant la personne à qui le nouveau mot de passe doit être délivré.
Données de licence	Fournissez les informations de licence à propos de votre cellule Data Protector.
Gestionnaire de cellule actuel	Fournissez les informations nécessaires concernant l'actuel Gestionnaire de cellule.
Nouveau Gestionnaire de cellule	Fournissez les informations nécessaires concernant votre nouveau Gestionnaire de cellule.
Numéro de commande	Saisissez le *Numéro de commande* imprimé sur le *Certificat.* Le *Numéro de commande* est nécessaire pour vérifier que vous êtes en droit de demander un mot de passe permanent.
Adresse IP	Ce champ définit le système pour lequel le *Centre de délivrance de mot de passe* générera les mots de passe. Au cas où vous voulez utiliser la gestion de licence centralisée (environnement MoM uniquement) alors ce système doit être le système de Gestionnaire MoM. Si le Gestionnaire de cellule dispose de plusieurs cartes LAN, vous pouvez saisir n'importe laquelle des adresses IP. Micro Focus recommande que vous saisissiez la première. Si vous avez Data Protector dans un environnement Serviceguard ou Microsoft Cluster, saisissez l'adresse IP de votre serveur virtuel. Pour plus d'informations sur les clusters, reportez-vous au *Aide de Data Protector*.
Les numéros de fax du *Centre de délivrance de mot de passe*	Pour des informations de contact, reportez-vous au *Certificat* distribué avec votre produit.

Type de licence produit	Dans les champs près des *Numéros de produit*, saisissez la quantité de licences que vous voulez installer sur ce Gestionnaire de cellule. La quantité peut être la totalité ou bien un sous-ensemble des licences achetées avec le *Numéro de commande*.

Vérification du mot de passe

Utilisation de l'interface utilisateur graphique

Pour vérifier si 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 **Licences**.
2. Cliquez sur l'onglet **Licences**. Toutes les licences installées sont affichées. Cliquez sur l'onglet **Infos mots de passe** pour voir les détails sur les mots de passe valides installés. Les mots de passe invalides seront marqués comme expirés ou supprimés.

   Toute la fenêtre pop-up ainsi que les colonnes individuelles sont redimensionnables.

Utilisation de l'interface de ligne de commande

Pour vérifier si le mot de passe pour la licence que vous avez installée est correct, utilisez la commande suivante :

```
omnicc -password_info
```

Cette commande affiche les licences installées. Si le mot de passe saisi est incorrect, il est listé avec la remarque `Password could not be decoded.`

Trouver le nombre de licences installées

Utilisation de l'interface utilisateur graphique

Une fois que vous avez installé un mot de passe permanent, vous pouvez vérifier le nombre de licences installées sur le Gestionnaire de cellule:

1. Démarrez Data Protector Manager.
2. Dans la barre du menu, cliquez sur **Aide**, puis **Licences...**. La fenêtre A propos de Manager s'ouvrira, affichant les licences installées.

Utilisation de l'interface de ligne de commande

Si vous utilisez la ligne de commande, procédez comme suit :

1. Identifiez-vous sur Gestionnaire de cellule.
2. Exécuter la commande suivante :

   ```
   omnicc -query
   ```

Un tableau listant les licences actuellement installées s'affichera.

Déplacer les licences vers un autre système Gestionnaire de cellule

Vous devez contacter le *Centre de délivrance de mot de passe* dans tous les cas suivants :

- Si vous souhaitez déplacer le Gestionnaire de cellule vers un autre système.
- Si vous prévoyez de déplacer une licence, installée sur un Gestionnaire de cellule qui n'est pas utilisé actuellement dans la cellule, vers une autre cellule Data Protector.

> **REMARQUE :**
> Les licences de produit UNIX fonctionnent sur les plates-formes UNIX, Windows, et Novell NetWare, fournissant la fonctionnalité quelle que soit la plate-forme, tandis que les licences de produit Windows fonctionnent uniquement sur les plates-formes Windows, Novell NetWare et Linux.
>
> Une licence de Gestionnaire de cellule pour HP-UX peut être déplacée vers et fonctionne sur toute plate-forme de gestionnaire de cellule. Une licence de Gestionnaire de cellule pour Windows ou Linux ne peut être déplacée vers et ne fonctionne pas pour une plate-forme de gestionnaire de cellule HP-UX.
>
> Toutes les autres licences peuvent être déplacées vers une plate-forme de gestionnaire de cellule sans restrictions. Le type de plate-forme de gestionnaire de cellule n'implique aucune restriction sur la licence. Par exemple, une licence de lecteur Windows peut être installée sur un gestionnaire de cellule HP-UX, cependant elle ne peut être utilisée pour un lecteur connecté à un système UNIX.

Pour déplacer les licences d'une instance de Gestionnaire de cellule à une autre :

1. Remplissez le *Formulaire de déplacement de licence* pour chaque nouveau Gestionnaire de cellule et envoyez-le au *Centre de délivrance de mot de passe.* Pour déplacer des licences pour les produits qui ne peuvent plus être achetés, vous devez utiliser les *Formulaires de déplacement de licence* délivrés avec la précédente version du produit. Voir Data Protector formulaires de licence, Page 307.

   Sur le formulaire, vous devez spécifier le nombre de licences que vous souhaitez déplacer depuis le Gestionnaire de cellule existant.

   En variante, rendez-vous sur le site web du centre de délivrance de mot de passe (https://software.microfocus.com/fr-fr/legal/software-licensing) et initiez le déplacement de licence en ligne.
2. Supprimez le fichier suivant :

   Systèmes Windows :

   données_programme_Data_Protector\config\server\cell\lic.dat

   Systèmes UNIX :

   /etc/opt/omni/server/cell/lic.dat
3. Dès que vous avez rempli et envoyé le *Formulaire de déplacement de licence* au *Centre de délivrance de mot de passe (PDC)*, vous êtes légalement obligé d'effacer tous les mots de passe Data Protector de l'actuel Gestionnaire de cellule.
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 l'actuel Gestionnaire de cellule si les licences sont laissées sur l'actuel Gestionnaire de cellule. Ce nouveau mot de passe remplace l'actuel Gestionnaire de cellule.

Chapitre 9: Dépannage des problèmes d'installation et de mise à jour

Ce chapitre contient des informations spécifiques aux problèmes liés à l'installation. Pour plus d'informations sur le dépannage, reportez-vous à la section *Guide de dépannage Data Protector*.

Problèmes de résolution de noms en installant le Gestionnaire de cellule Windows

Au cours de l'installation du Gestionnaire de cellule Data Protector sur Windows, Data Protector détecte et vous avertit si le DNS ou le fichier LMHOSTS n'est pas paramétré comme prévu. De plus, Data Protector vous notifie si le protocole TCP/IP n'est pas installé sur votre système.

Problème

La résolution de nom échoue en utilisant DNS ou LMHOSTS

Si la résolution de nom échoue, le message "`error expanding hostname`" s'affiche et l'installation est interrompue.

- Si vous rencontrez un problème de résolution en utilisant le DNS, vous obtenez un message d'alerte à propos de votre configuration DNS actuelle.
- Si vous rencontrez un problème de résolution en utilisant un fichier LMHOSTS, vous obtenez un message d'alerte à propos de votre configuration du fichier LMHOSTS actuelle.
- Si vous n'avez configuré ni DNS ni LMHOSTS, vous obtenez un message d'alerte pour activer la résolution DNS ou LMHOSTS dans le dialogue de propriétés TCP/IP.

Action

Vérifiez votre configuration de fichier DNS ou LMHOSTS ou activez-la. Voir Vérification des connexion DNS dans la cellule Data Protector, Page suivante.

Problème

Le protocole TCP/IP n'est pas installé ni configuré sur votre système

Data Protector utilise le protocole TCP/IP pour les communications réseau; il doit être installé et configuré sur chaque client dans la cellule. Sinon, l'installation est abandonnée.

Action

Vérifiez la configuration TCP/IP. Pour plus d'informations, voir Changer le port Inet par défaut Data Protector, Page 354.

Vérification des connexion DNS dans la cellule Data Protector

DNS (Domain Name System) est un service de nom pour les hôtes TCP/IP. Le DNS est configuré avec une liste d'hôtes et d'adresses IP, permettant aux utilisateurs de spécifier les systèmes à distance par les noms d'hôtes plutôt que par les adresses IP. DNS assure une communication adéquate parmi les membres de la cellule Data Protector.

Si le DNS n'est pas correctement configuré, les problèmes de résolution de nom peuvent survenir dans la cellule Data Protector et les membres ne pourront pas communiquer les uns avec les autres.

Data Protector fournit la commande omnicheck`omnicheck` pour vérifier les connexions DNS parmi les membres de la cellule Data Protector. Bien que toutes les connexion possibles dans la cellule peuvent être vérifiées avec cette commande, il suffit de vérifier les connexions suivantes, qui sont essentielles dans la cellule Data Protector :

- Gestionnaire de cellule vers tout autre membre de la cellule et vice-versa
- L'Agent de support vers tout autre membre de la cellule et vice-versa

Utilisation de la commande omnicheck

Limites

- La commande vérifie les connexions parmi les membres de la cellule uniquement; elle ne vérifie pas les connexions DNS en général.

Le synopsis de la commande omnicheck est :

```
omnicheck -dns [-host Client | -full] [-verbose]
```

Vous pouvez vérifier les connexions DNS dans la cellule Data Protector en utilisant différentes options :

- Pour vérifier que le Gestionnaire de cellule et chaque Agent de support dans la cellule résout correctement les connexions DNS pour chaque client Data Protector dans la cellule et vice-versa, exécutez :

  ```
  omnicheck -dns [-verbose]
  ```
- Pour vérifier que le client particulier Data Protector résout correctement les connexions DNS pour chaque client Data Protector dans la cellule et vice-versa, exécutez :

  ```
  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 :

  ```
  omnicheck -dns -full [-verbose]
  ```

Lorsque l'option `[-verbose]` est spécifiée, la commande retourne tous les messages. Si cette option n'est pas définie (ce qui le cas par défaut), seuls les messages liés à des vérifications ayant échoué s'affichent.

Pour plus d'informations, voir la page du manuel `omnicheck`.

Messages de retour, bas dresse la liste des messages de retour pour la commande `omnicheck`. Si le message de retour indique un problème de résolution de DNS, reportez-vous au chapitre "Dépannage de réseau et Communication" du *Guide de dépannage Data Protector*.

Messages de retour

Message de retour	Signification
client_1 cannot connect to *client_2*	Expiration de la connexion vers *client_2*.
client_1 connects to *client_2*, but connected system presents itself as *client_3*	Le fichier *%SystemRoot%*\System32\drivers\etc\hosts/etc/hosts (systèmes UNIX) sur le *client_1* n'est pas configuré correctement ou le nom d'hôte de *client_2* ne correspond pas à son nom DNS.
client_1 failed to connect to *client_2*	*client_2* est soit hors d'atteinte (par exemple, déconnecté) ou bien le fichier *%SystemRoot%*\System32\drivers\etc\hosts(systèmes Windows) ou /etc/hosts(systèmes UNIX) sur le *client_1* n'est pas correctement configuré.
checking connection between *client_1* and *client_2*	
all checks completed successfully.	
number_of_failed_checks checks failed.	
client is not a member of the cell.	
client contacted, but is apparently an older version. Hostname is not checked.	

Problèmes généraux de dépannage

Problème

L'un des messages d'erreur suivants est signalé

- The Windows Installer Service could not be accessed.
- This application must be installed to run.
- This patch package could not be opened.
- The system cannot open the device or file specified.

Après l'installation ou la mise à niveau de Data Protector, Windows peut signaler que certaines applications ne sont pas installées ou qu'une réinstallation est nécessaire.

La raison tient à une erreur dans la procédure de mise à jour de Microsoft Installer de . Les informations de données de la version 1.x de Microsoft Installer ne sont pas migrées vers la version 2.x de Microsoft Installer version 2.x que Data Protector installe sur l'ordinateur.

Action

Sur la façon de résoudre le problème, reportez-vous à l'article Q324906 dans la Base de connaissances Microsoft.

Problème

L'installation Gestionnaire de cellule sur un système Windows, qui ne fait pas partie d'un domaine Windows, échoue

Le message d'erreur suivant est reporté :

```
Setup is unable to match the password with the given account name.
```

Actions

Deux solutions sont disponibles :

- Faites appartenir le système Windows, sur lequel vous installez le Gestionnaire de cellule, à un domaine.
- Utilisez le compte administrateur local pour le service CRS.

Problème

L'erreur suivante est renvoyée :

```
msvcr90.dll file is not found
```

La bibliothèque `MSVCR90.dll` (en majuscules) est introuvable, car seul le fichier `msvcr90.dll` (en minuscules) est disponible sur le partage réseau. `MSVCR90.dll` Et `msvcr90.dll` étant traités comme des fichiers différents, `setup.exe` ne parvient pas à trouver le fichier `dll` approprié.

Action

Renommez le fichier `msvcr90.dll` (en minuscules) en `MSCVCR90.dll` (en majuscules) ou reconfigurez le partage réseau pour qu'il ne soit pas sensible à la casse.

Problème

L'annulation de l'installation ne désinstalle pas les composants déjà installés

Si vous annulez l'installation de Data Protector alors que certains composants ont déjà été installés, Data Protector L'installation se termine avec une erreur.

Action

Désinstallez manuellement les composants déjà installés après avoir annulé l'installation.

Problème

L'erreur suivante est renvoyée

```
"too many open files" error
```

Le CRS (Cell Request Server) ajuste sa `ulimit` pour prendre en charge un grand nombre de fichiers ou sockets ouverts, ce qui est généralement suffisant. Si vous rencontrez des erreurs de type "trop de fichiers ouverts", vous devez régler les paramètres du système d'exploitation.

Action

Les paramètres du système d'exploitation couvrent deux aspects :

- Ils changent la limite pour les fichiers ou sockets ouverts.
- Ils influencent les performances lorsque de nombreuses connexions de socket sont présentes.

La liste suivante n'est pas exhaustive. Pour plus d'informations, consultez la documentation du système d'exploitation.

HP-UX

Le nombre maximum de fichiers ouverts est défini par les variables du noyau.

Pour le configurer, utilisez `kctune variable=value`.

Pour l'afficher, utilisez `kctune -v variable` ou `kcusage`.

variable	par défaut	valeurs valides	note
maxfiles	2048	32 à 1 048 576 <= maxfiles_lim	Nombre maximum initial (logiciel) de descripteurs de fichier par processus ulimit –Sn
maxfiles_lim	4096	32 à 1 048 576 >= maxfiles <= nfile/2	Nombre maximum initial (matériel) de descripteurs de fichier par processus ulimit –Hn
nfile	65 536	2048 … 2,147,483,647 >= 2*maxfiles_lim	Nombre maximum de descripteurs de fichier (à l'échelle du système) **Remarque :** "ulimit –Hn nnn" réussit même si nnn > nfile/2

Réglez aussi les paramètres réseau avec `ndd` pour un grand nombre de sockets, comme décrit ici :

```
ndd -h tcp_time_wait_interval

ndd -h tcp_fin_wait_2_timeout

ndd -h /dev/tcp tcp_smallest_anon_port

vi /etc/rc.config.d/nddconf
```

Linux

Les paramètres de noyau sont enregistrés à l'emplacement suivant :

```
/etc/sysctl.conf
```

Vous pouvez modifier le fichier `sysctl.conf` ou appeler `sysctl -w name=value`. Vous pouvez également charger le noyau avec `sysctl -p` ou modifier son fichier `procfs` correspondant. Par exemple, la variable `fs.file-max` correspond à `/proc/sys/fs/file-max`.

REMARQUE :
Les valeurs par défaut dépendent de la mémoire disponible.

Variable	Remarque
fs.file-max	Le nombre maximum de descripteurs de fichier (à l'échelle du système).
net.core.somaxconn	La longueur maximale à laquelle la file d'attente de connexions en attente pour le socket d'écoute peut augmenter.
connecteur net.ipv4.tcp_max_ syn_backlog	Le nombre maximum de requêtes de connexion mémorisées qui n'ont pas encore reçu un accusé de réception du client de connexion.

En outre, les valeurs par défaut pour les limites de prétraitement sont stockées à l'emplacement suivant :

`/etc/limits.conf`

(OU)

`/etc/security/limits.conf`

Dépannage d'installation sur les systèmes UNIX

Problème

Installation à distance d'échecs de clients UNIX

L'installation à distance ou la mise à jour d'un client UNIX échoue avec le message d'erreur suivant :

```
Installation/Upgrade session finished with errors.
```

En installant ou en mettant à jour des clients UNIX à distance, l'espace disque disponible sur un système client dans le dossier `/tmp` doit avoir au moins la taille du plus grand paquet utilisé pour l'installation. Sur les systèmes client Solaris, la même quantité d'espace disque doit également être disponible dans le dossier `/var/tmp`.

Action

Vérifiez si vous avez assez d'espace disque dans les répertoires mentionnés ci-dessus et redémarrez la procédure d'installation ou de mise à jour.

Pour les conditions d'espace disque requises, consultez Installer des clients Data Protector, Page 54.

Problème

Problèmes avec l'installation d'un client HP-UX

En ajoutant un nouveau client HP-UX à une cellule Data Protector, le message d'erreur suivant est affiché :

```
/tmp/omni_tmp/packet: you do not have the required permissions to perform this SD
function.....
```

```
Access denied to root at to start agent on registered depot /tmp/omni_tmp/packet.
No insert permission on host.
```

Action

Arrêtez le daemon `swagent` et redémarrez-le soit en interrompant le processus puis en le redémarrant en lançant la commande `/opt/omni/sbin/swagentd` soit en lançant la commande `/opt/omni/sbin/swagentd -r`.

Assurez-vous que vous avez un hôte local, une entrée loopback dans les fichiers hôtes (`/etc/hosts`).

Problème

Problèmes avec l'installation d'un client Mac OS X

An ajoutant un client Mac OS X à une cellule Data Protector, le processus `com.hp.omni` n'est pas démarré.

Action

Sur Mac OS X, `launchd` est utilisé pour démarrer le processus `com.hp.omni`.

Pour démarrer le service, allez à :

```
cd /usr/omni/newconfig/System/Library/LaunchDaemons
```

Exécutez :

```
launchctl load com.hp.omni
```

Problème

Processus Inet ne peut être démarré après l'installation du Gestionnaire de cellule UNIX the UNIX Gestionnaire de cellule

En démarrant le Gestionnaire de cellule, l'erreur suivante est affichée :

```
ERROR: Cannot start "omniinet" service, system error: [1053] Unknown error 1053.
```

Action

Vérifiez que le service `inetd` ou `xinetd` est en cours d'exécution :

Systèmes HP-UX : `ps -ef | grep inetd`

Systèmes Linux : `ps -ef | grep xinetd`

Pour démarrer le service, exécuter :

Systèmes HP-UX : `/usr/sbin/inetd`

Systèmes Linux : `rcxinetd start`

Problème

L'installation push sur les clients Linux avec des informations d'identification valides échoue avec le message suivant :

```
[Critical] <iwf1114165.hpeswlab.net>  SSH configuration failed. Either the
credentials were wrong or some error occured.
```

```
<iwf1114165.hpeswlab.net> : Skipped  0%
```

```
[Critical] <iwf1114165.hpeswlab.net>  Error connecting to client
iwf1114165.hpeswlab.net

Skipping client!

[Normal]  Installation session finished on Mon 14 Nov 2016 03:13:52 PM IST.

Finished installation.
```

Action

Vérifiez que l'authentification par mot de passe est activée pour le service `ssh` sur les clients Linux. Dans le cas contraire, suivez ces étapes :

1. Activez l'authentification en ajoutant ce qui suit au fichier `ssh config` :

   PasswordAuthentication yes
2. Redémarrez le service `ssh`.

Dépannage d'installation sur les systèmes Windows

Problème

Installation à distance d'échecs de clients Windows

L'installation à distance d'un client Data Protector vers un système Windows échoue et reporte le message d'erreur suivant :

```
[Normal] Connecting to client computer.company.com...

[Normal] Done.

[Normal] Installing the Data Protector bootstrap service on client
computer.company.com...

[Critical] Cannot connect to the SCM (Service Control Manager) on client
computer.company.com: [5] Access is denied.
```

Action

1. Sur le système Serveur d'installation, exécutez la commande suivante pour marquer un compte utilisateur depuis le groupe utilisateur des Administrateurs d'un système fonctionnant en local qui doit être utilisé par le Serveur d'installation au cours de l'installation à distance :

   `omniinetpasswd –inst_srv_user` *`User@Domain`*

   Notez que le compte utilisateur doit déjà avoir été ajouté à la configuration Inet locale. Pour plus de détails, voir la description de la commande `omniinetpasswd` dans le document *Guide de référence de l'interface de ligne de commande Data Protector*.
2. Démarrez à nouveau l'installation à distance du client Data Protector.

Problème

Installation à distance d'échecs de clients Windows (Windows XP)

Lorsqu'un système Windows XP est un membre d'un groupe de travail et que le paramètre de stratégie de sécurité Simple File Sharing est activé, les utilisateurs tentant d'accéder à ce système à travers le

réseau sont forcés d'utiliser le compte Invité. Au cours de l'installation à distance d'un client Data Protector, Data Protector demande de manière répétée un nom d'utilisateur et un mot de passe valides parce que les droits administrateur sont nécessaires pour l'installation à distance.

Action

Désactivez Simple File Sharing: dans Windows XP, ouvrez **Windows Explorer** ou **Mon Ordinateur**, cliquez sur le menu **Outils**, cliquez **Options dossier**, cliquez sur l'onglet **Voir**, puis décochez la case **Utiliser simple file sharing (Recommandé)**.

La stratégie Simple File Sharing est ignorée :

- lorsque l'ordinateur est un membre du domaine
- si le paramètre de politique de sécurité `Network access: Sharing and security model for local accounts` est défini sur `Classic: Local users authenticate as themselves`

Problème

La vérification de signature numérique peut échouer, si les systèmes Windows 7 ou Windows 2008 R2 sont déconnectés.

La vérification de signature numérique échoue avec le message d'erreur suivant :

```
[Critical] <computer.company.com> [70:32] Digital Signature verification of the install kit failed.
```

Action

Sélectionnez l'une des méthodes suivantes :

- Activez la connexion internet et attendez jusqu'à ce que les certificats appropriés sont importés automatiquement dans le root dédié et les autorités de certificat intermédiaires.

  (ou)
- Reportez-vous aux articles suivants pour comprendre comment mettre à niveau les certificats root dédiés sur les systèmes déconnectés :

  https://support.microsoft.com/en-us/kb/3004394

  https://support.microsoft.com/en-us/kb/2813430

Problème

En installant Cell Manager, le service Application Server échoue à démarrer

Le service Application Server échoue à démarrer avec le message

```
Timeout reached before Data Protector Application Server started.
```

L'erreur suivante est enregistrée dans le fichier journal résumant l'installation :

```
Caused by: org.jboss.as.cli.
CommandLineException: The controller is not available at localhost:9999
```

Le processus d'installation ne peut pas accéder à divers utilitaires, car la variable d'environnement système PATH ne contient pas le répertoire `%SystemRoot%\system32`.

Action

Ajoutez le répertoire `%SystemRoot%\system32` à la variable PATH.

REMARQUE :
Les fichiers suivants sont placés (selon les composants sélectionnés) dans le dossier `%SystemRoot%\system32` sur les systèmes Windows :

`BrandChgUni.dll`	Il s'agit d'une bibliothèque de ressource. Elle est utilisée uniquement en interne ; cependant, elle contient également le chemin vers les paramètres de registre, elle doit donc être située dans un emplacement bien connu où les bibliothèques d'intégration peuvent y accéder.
`ob2informix.dll`	Cette bibliothèque est utilisée pour intégrer la base de données Informix Server.
`snmpOB2.dll`	Cette bibliothèque est utilisée pour implémenter les pièges du système SNMP.

Vérification de l'installation client de Data Protector

La vérification de l'installation client Data Protector consiste à :

- Vérifier la configuration DNS sur le Gestionnaire de cellule et les systèmes client, et s'assurer que les résultats de la commande `omnicheck -dns` sur le Gestionnaire de cellule et les système client correspondent au système spécifié.
- Vérifier les composants logiciels installés sur le client.
- Comparer la liste de fichiers nécessaire pour un certain composant logiciel qui doit être installé avec les fichiers installés sur le client.
- Vérifier la somme de contrôle pour chaque fichier en lecture seule pour un certain composant logiciel.

Conditions préalables

Un Serveur d'installation doit être disponible pour le type de système client system (UNIX, Windows) que vous sélectionnez.

Limite

Pour vérifier une installation de Data Protector utilisant l'interface graphique utilisateur Data Protector :

1. Dans la liste de contexte, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, développez l'élément **Clients**, faites un clic droit sur le système Gestionnaire de cellule, puis cliquez sur **Vérifier installation** pour ouvrir l'assistant.
3. Suivez l'assistant pour vérifier l'installation des systèmes dans la cellule. La fenêtre de vérification de l'installation s'ouvre, affichant les résultats de l'installation.

   Pour plus d'informations, voir *Aide de Data Protector*.

Si votre installation n'a pas réussi, reportez-vous à Utilisation des fichiers journaux, Page 340.

Sur la manière de vérifier l'installation de systèmes UNIX utilisant le CLI Data Protector, reportez-vous à la page `ob2install`.

Mise à jour de dépannage

Problème

La mise à jour échoue si la version précédente du produit est installée sur un chemin d’accès long

Data Protector ne prend pas en charge l'installation du Gestionnaire de cellule vers un cheminement long de plus de 80 caractères. En conséquence, la mise à jour échoue.

Action

1. Copiez le script `omnimigrate.pl` du package d'installation, à partir du répertoire `x8664\tools\Upgrade`, vers un répertoire temporaire, par exemple `c:\temp`.
2. Utilisez la commande `omnimigrate` pour exporter l'IDB :

   ```
   perl c:\temp\omnimigrate.pl -export -shared_dir c:\output
   ```

   Utilisez la version Perl qui fait partie de l'installation de Data Protector et qui réside dans le répertoire de commandes par défaut.
3. Supprimez la version précédente de Data Protector, mais conservez la configuration et la base de données. Ne supprimez pas le répertoire *données_programme_Data_Protector*`\db40`.
4. Installez Data Protector 10.00. Assurez-vous que le cheminement d'installation comporte moins de 80 caractères.
5. Arrêtez tous les services de Data Protector :

   ```
   omnisv –stop
   ```
6. Copiez les fichiers de l'ancien répertoire *données_programme_Data_Protector*`\db40` (laissé après la suppression de la version précédente de Data Protector) vers le nouveau dossier *données_programme_Data_Protector*`\db40`. Assurez-vous que vous ne déplacez *pas* les répertoires DCBF.
7. Copiez la configuration de l'ancien dossier *données_programme_Data_Protector*`\Config\Server` vers le nouveau :
   a. Copiez l'ancien répertoire de configuration vers le nouveau, mais gardez les anciens fichiers. Ne copiez pas les fichiers du répertoire *données_programme_Data_Protector*`\Config\Server\install`.
   b. Si vous souhaitez conserver la configuration de la cellule (clients, Serveur d'installation), copiez et remplacez les fichiers *données_programme_Data_Protector*`\Config\Server\cell\cell_info` et *données_programme_Data_Protector*`\Config\Server\cell\installation_servers`.
8. Fusionnez la nouvelle notification et le fichier d'options globales :
   a. Pour fusionner les notifications, exécutez l'outil `omninotifupg.exe` :

      ```
      omninotifupg.exe -quiet
      ```
   b. Pour fusionner le fichier des options globales, exécutez :

      ```
      mrgcfg.exe –global -except BackupDeviceIdle -rename
      DbFVerLimit=DbFnamesDatLimit,SessSucessfulWhenNoObjectsBackedUp
      =SessSuccessfulWhenNoObjectsBackedUp
      ```

Alternativement, vous pouvez fusionner manuellement le fichier d'options globales de l'ancienne installation.

9. Démarrez les services Data Protector:

   ```
   omnisv -start
   ```

10. Importez l'IDB vers la nouvelle installation. Exécutez :

    ```
    omnimigrate.pl -import -shared_dir c:\output -force
    ```

Problème

La mise à jour échoue si la version précédente du produit est installée avec des caractères non pris en charge

Data Protector ne prend pas en charge l'installation de Cell Manager vers un cheminement qui :

- contient des caractères non-ASCII
- contient les caractères "@ " ou "# "
- contient un répertoire qui se termine avec le caractère "!"

En conséquence, la mise à jour échoue.

Action

1. Copiez le script `omnimigrate.pl` du package d'installation, à partir du répertoire `x8664\tools\Upgrade`, vers un répertoire temporaire, par exemple `c:\temp`.
2. Créez deux répertoires avec des noms ASCII par exemple :

   ```
   c:\output\cdb
   ```

   ```
   c:\output\mmdb
   ```

3. Exportez les MMDB et CDB :

   ```
   omnidbutil -writedb -cdb c:\output\cdb -mmdb c:\output\mmdb
   ```

   Ce processus peut prendre quelques minutes. Vous pouvez arrêter le processus `omnidbutil` en utilisant **Ctrl+C** lorsqu'il commence à exporter les noms de fichier car les données ne sont pas nécessaires pour la mise à jour.

4. Utilisez la commande `omnimigrate` pour exporter l'IDB :

   ```
   perl c:\temp\omnimigrate.pl -exportNonASCII -shared_dir c:\output
   ```

   Utilisez la version Perl qui fait partie de l'installation de Data Protector et qui réside dans le répertoire de commandes par défaut.

5. Créez un fichier de jeu de caractères ANSI, `c:\output\old_cm`. Ce fichier devrait contenir les deux lignes suivantes :

   ```
   OLDCM_SHORTNAME=OldCmName
   OLDCM_ENDIANNESS=LITTLE_ENDIAN
   ```

   Remplacez *OldCmName* avec l'abréviation de Gestionnaire de cellule.

6. Supprimez la version précédente de Data Protector, mais conservez la configuration et la base de données. Ne supprimez pas le répertoire *données_programme_Data_Protector*\db40.
7. Installez Data Protector. Assurez-vous que le cheminement d'installation ne contient aucun caractère non-ASCII.
8. Arrêtez tous les services de Data Protector :

```
omnisv –stop
```

9. Copiez les fichiers de l'ancien répertoire *données_programme_Data_Protector*\db40 (laissé après la suppression de la version précédente de Data Protector) vers le nouveau dossier *données_programme_Data_Protector*\db40. Assurez-vous que vous ne déplacez *pas* les répertoires DCBF.
10. Copiez la configuration de l'ancien dossier *données_programme_Data_Protector*\Config\Server vers le nouveau :
    a. Copiez l'ancien répertoire de configuration vers le nouveau, mais gardez les anciens fichiers. Ne copiez pas les fichiers du répertoire *données_programme_Data_Protector*\Config\Server\install.
    b. Si vous souhaitez conserver la configuration de la cellule (clients, Serveur d'installation), copiez et remplacez les fichiers *données_programme_Data_Protector*\Config\Server\cell\cell_info et *données_programme_Data_Protector*\Config\Server\cell\installation_servers.
11. Fusionnez la nouvelle notification et le fichier d'options globales :
    a. Pour fusionner les notifications, exécutez l'outil omninotifupg.exe :

    ```
    omninotifupg.exe -quiet
    ```

    b. Pour fusionner le fichier des options globales, exécutez :

    ```
    mrgcfg.exe –global -except BackupDeviceIdle -rename
    DbFVerLimit=DbFnamesDatLimit,SessSucessfulWhenNoObjectsBackedUp
    =SessSuccessfulWhenNoObjectsBackedUp
    ```

    Alternativement, vous pouvez fusionner manuellement le fichier d'options globales de l'ancienne installation.
12. Démarrez les services Data Protector:

    ```
    omnisv -start
    ```

13. Importez l'IDB vers la nouvelle installation. Exécutez :

    ```
    omnimigrate.pl -import -shared_dir c:\output -force
    ```

Problème

Le processus de mise à jour est abandonné si l'ancienne IDB (basée sur Raima DB) est corrompue

Au cours de la mise à jour, les champs corrompus suivants dans l'IDB sont détectés et corrigés :

- Le support blocks_used est défini sur 0
- Le support blocks_total est défini sur blocks_used
- Le pool media_age_limit est fixé sur la valeur par défaut (media_age_limit pour le pool par défaut avec la même classe de support)
- Le pool media_overwrite_limit est fixé sur la valeur par défaut (media_overwrite_limit pour le pool par défaut avec la même classe de support)

Cependant, si aucun autre champ dans l'IDB n'est corrompu, la mise à jour est abandonnée.

Action

Revenez à l'installation de l'ancienne version de Data Protector :

1. Supprimez la version actuelle de Data Protector.
2. Réinstallez la version précédente de Data Protector.
3. Restaurez l'ancienne IDB.

Avant de tenter une autre mise à jour, vous devez réparer l'ancienne IDB. Contactez assistance clientèle pour obtenir de l'aide.

Problème

Après la mise à niveau, une erreur déclenche l'échec de `omnidbcheck -bf`

Dans les précédentes versions de Data Protector, `omnidbcheck -bf` ne rapportait pas correctement les erreurs dues à l'inconsistance entre la taille réelle et la taille du titre du support dans les fichiers binaires DC.

`omnidbcheck -bf` rapporte correctement toutes les erreurs qui peuvent exister dans l'IDB avant la mise à jour.

Action

Si certains fichiers binaires DC sont endommagés, vous pouvez les supprimer et les recréer en important les supports avec un niveau de journalisation approprié. À la suite de cette opération, certaines positions de support désignent des fichiers binaires inexistants et un message d'erreur s'affiche lors de l'exploration des systèmes de fichiers correspondants.

1. À partir des résultats de la commande `omnidbcheck -dc`, identifiez l'ID du support du fichier binaire DC endommagé.
2. Exécutez la commande `omnimm -media_info` *`medium-id`* pour obtenir les autres attributs du support, comme son étiquette et le pool auquel il appartient.
3. Identifiez le fichier binaire DC du support concerné. Les fichiers binaires DC possèdent un nom au format suivant : *`MediumID_TimeStamp`*`.dat` (dans `MediumID`, les deux-points « : » sont remplacés par des traits de soulignement « _ »).
4. Supprimez les fichiers binaires DC endommagés.
5. Exécutez la commande `omnidbutil -fixmpos` pour rétablir la cohérence entre les positions de support (mpos) et les fichiers binaires.
6. Importez le catalogue à partir des supports afin de recréer les fichiers binaires.

   Pour plus d'informations, reportez-vous à *Aide de Data Protector* et *Guide de dépannage Data Protector* "gérer la corruption IDB mineure dans la partie DCBF". Contactez assistance clientèle pour obtenir de l'aide.

Problème

Le processus de mise à jour est abandonné si l'IDB Velois est corrompue

Au cours de la mise à jour, les champs corrompus suivants dans l'IDB sont détectés et corrigés :

- Le support `blocks_used` est défini sur `99`
- Le support `blocks_total` est défini sur `blocks_used`
- Le pool `media_age_limit` est fixé sur la valeur par défaut (`media_age_limit` pour le pool par défaut avec la même classe de support)
- Le pool `media_overwrite_limit` est fixé sur la valeur par défaut (`media_overwrite_limit` pour le pool par défaut avec la même classe de support)

Cependant, si aucun autre des champs suivants dans l'IDB n'est corrompu, la mise à jour est abandonnée.

Support : `LAST_SEGMENT`

Positions :

`SEQUENCE_NR`

`START_SEGMENT`

`START_OFFSET`

`LOG_LEVEL`

`DCBF_OFFSET`

`DCBF_NUMOFDIRS`

`DCBF_NUMOFITEMS`

`DCBF_SIZE`

Action

Revenez à l'installation de l'ancienne version de Data Protector :

1. Supprimez la version actuelle de Data Protector.
2. Réinstallez la version précédente de Data Protector.
3. Restaurez l'ancienne IDB.

Avant de tenter une autre mise à jour, vous devez réparer l'ancienne IDB. Contactez assistance clientèle pour obtenir de l'aide.

Problème

IDB et les fichiers de configuration ne sont pas disponibles après mise à jour

Après la mise à jour de Gestionnaire de cellule d'une version précédente, l'IDB et tous les fichiers de configuration ne sont pas disponibles. Ceci se produit si la procédure de mise à jour a été interrompue pour une raison quelconque.

Action

Restaurez Data Protector de la sauvegarde effectuée avant la mise à jour, éliminez la raison de l'interruption et démarrez à nouveau la mise à jour.

Problème

Les anciens patchs Data Protector ne sont pas supprimés après la mise à jour

Les anciens patchs Data Protector sont listés parmi les programmes si la commande `swlist` est lancée après que la mise à jour de Data Protector est terminée. Les patchs ont été supprimés de votre système au cours de la mise à jour, mais ils sont restés dans la base de données de logiciels.

Pour vérifier quels patchs Data Protector sont installés, consultez Vérifier les correctifs Data Protector à l'aide de l'interface utilisateur graphique, Page 226.

Action

Pour supprimer les anciens patchs de la base de données sw, lancez la commande suivante :

`swmodify -u`*`patch`*`.\*`*`patch`*

Par exemple, pour supprimer un patch `PHSS_30143` de la base de données de logiciels, lancez la commande suivante :

```
swmodify -u PHSS_30143.\* PHSS_30143
```

Problème

La mise à jour d'un client Agent de support qui utilise la StorageTek Library provoque des problèmes de connectivité

Après la mise à jour de Data Protector, le composant d'Agent de support sur un système qui utilise la StorageTek Library, la connectivité à la bibliothèque est perdue et les sessions de Data Protector qui impliquent la bibliothèque peuvent s'arrêter de répondre ou bien s'interrompre de manière anormale.

Action

Le redémarrage du service d'assistance ou daemon de StorageTek Library peut résoudre le problème :

Systèmes Windows : En utilisant l'outil administratif Service, 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` *`ACSLS_hostname`*, où *ACSLS_hostname* est le nom du système sur lequel le logiciel de bibliothèque à système de cartouche automatisé est installé.

Systèmes AIX : Exécutez les commandes `/usr/omni/acs/ssi.sh stop` et `/usr/omni/acs/ssi.sh start` *`ACSLS_hostname`*, où *ACSLS_hostname* est le nom du système sur lequel le logiciel de bibliothèque à système de cartouche automatisé est installé.

Problème

Après la mise à jour de Data Protector 10.00 ou d'une version ultérieure, lorsque vous effectuez une opération de restauration, un message d'erreur DCBF apparaît. Dans l'Interface graphique utilisateur de Data Protector, dans le contexte de restauration, lorsque vous sélectionnez un objet et essayez de parcourir des fichiers, le message suivant apparaît :

```
[12:10907] Invalid format of detail catalog binary file.
```

Cependant, `omnidbcheck -dc` ne rapporte AUCUNE erreur, puisque les fichiers DCBF ne sont PAS vraiment corrompus. Ceci a lieu en raison d'un décalage de version, comme deux fichiers de versions différentes sont lus.

Action

Option 1 : Allez dans le contexte Restaurer Sessions et essayez de restaurer les fichiers seuls.

Option 2 : Exportez/importez le support, le catalogue DCBF est recréé. Pour plus d'informations, reportez-vous aux sections "*Importer un Support*" et "*Exporter un Support*" de *Aide de Data Protector.*

Option 3 : Migration de catalogue. `perl omnimigrate.pl -start_catalog_migration`

> **REMARQUE :**
> Une fois la migration complète du catalogue effectuée (après qu'il n'y ait pas d'anciens catalogues), modifiez la variable globale `SupportOldDCBF` en `0`.

Problème

Après la mise à jour vers la version Data Protector de 10.00 ou suivantes, si vous sélectionnez un disque individuel, qui est sauvegardé en utilisant Data Protector 7.03, pour la restauration, alors l'Interface graphique de Data Protector affiche les messages d'erreur suivants :

```
Object scsi0:<disk number> does not have version information. Most probably backup of this object was not completed - restore will not be possible.
```

```
There is a problem with restore object '<VCenter host> Virtual Environment [<Data center>]'. It might not have any version information or there is some other conflict. Restore was aborted.
```

Action

Sélectionnez la machine virtuelle complète à restaurer.

Problème

La migration de la planification échoue pendant la mise à niveau

Action

Si la migration des planifications échoue au cours du processus de mise a niveau, vous pouvez exécuter manuellement la commande suivante pour réussir la migration des planifications existantes vers le nouveau planificateur :

```
omnidbutil -migrate_schedules
```

Dépannage à distance de mise à jour sur les systèmes Windows

Problème

Erreur en démarrant le processus de paramétrage

En utilisant la fonctionnalité d'installation à distance Data Protector pour mettre à jour des clients Windows, vous obtenez l'erreur suivante :

```
Error starting setup process, err=[1326] Logon failure: unknown user name or bad password.
```

Le problème est que le service `Data Protector Inet` sur l'ordinateur à distance fonctionne sous un compte utilisateur qui n'a pas accès au partage de OmniBack sur l'ordinateur Serveur d'installation. Il s'agit probablement d'un utilisateur local.

Action

Passez de l'utilisateur du service `Data Protector Inet` à un utilisateur qui peut accéder au partage Data Protector.

Problème

Le Data ProtectorCell Request Server (CRS) ne démarre pas après la mise à niveau

Le message d'erreur suivant s'affiche lorsque vous démarrez manuellement le CRS :

```
Windows could not start the Data Protector CRS on Local Computer.

For more information, review the System Event Log. If this is a non-Microsoft
service, contact the service vendor, and refer to service-specific error code 1007.
```

Le message d'erreur suivant apparaît après l'installation :

```
Timeout reached before Data Protector CRS started.
```

Action

- Arrêtez les services Data Protector à l'aide de la commande `omnisv stop` .
- Ouvrez le gestionnaire de tâches et fermez les processus Data Protector restants.
- Démarrez les services Data Protector à l'aide de la commande `omnisv start` .

Processus manuel pour la mise à jour locale sur des systèmes UNIX

Normalement, vous mettez à niveau Data Protector8.1 et version ultérieure sous UNIX Gestionnaire de cellule et Serveur d'installation en exécutant la commande `omnisetup.sh`, qui effectue une procédure de mise à jour automatisée. Cependant, vous pouvez aussi effectuer la mise à jour manuellement. Voir Mise à jour sur les systèmes HP-UX et Linux en utilisant les outils natifs., Page 349.

Après avoir mis à niveau le client manuellement, exécutez la commande `omnicc` suivante dans le Gestionnaire de cellule pour mettre à jour les informations du client :

```
omnicc –update_host [hostname] -accept_host
```

Pour mettre à jour toutes les informations client qui font partie de la cellule, exécutez la commande suivante :

```
omnicc –update_all -accept_host
```

Pour de plus amples informations sur la commande `omnicc`, consultez le guide *Guide de référence de l'interface de ligne de commande Data Protector*.

Utilisation des fichiers journaux

Si vous rencontrez des problème dans l'installation de Data Protector, vous pouvez examiner les fichiers journaux suivants pour déterminer votre problème :

- paramétrer fichiers journaux (Windows)
- système fichiers journaux (UNIX)
- Data Protector fichiers journaux

Savoir quels fichiers journaux vérifier en cas de problèmes d'installation dépend du type d'installation (locale ou à distance) et du système d'exploitation.

Installation en local

En cas de problèmes avec l'installation locale, vérifiez les fichiers journaux suivants :

HP-UX Gestionnaire de cellule:

- `/var/adm/sw/swinstall.log`
- `/var/adm/sw/swagent.log` (Pour plus de détails)

Linux Gestionnaire de cellule:

`/var/opt/omni/log/debug.log`

Client Windows (le système sur lequel le paramétrage fonctionne) :

- *Temp*`\SetupLog.log`
- *Temp*`\OB2DBG_`*did*`__setup_`*HostName*`_`*DebugNo*`_setup.txt` (Pour plus de détails)

  où :

  - *did* (ID de débogage) est l'identifiant du premier processus qui accepte les paramètres de débogage. Cet ID est utilisé comme ID pour la session de débogage. Tous les processus ultérieurs utiliseront cet ID.
  - *HostName* est le nom de l'hôte où le fichier trace est créé.
  - *DebugNo* est un numéro généré par Data Protector.

- *Temp*`\CLUS_DBG_`*DebugNo*`.TXT` (dans les environnements cluster)

L'emplacement du répertoire *Temp* est spécifié par la variable d'environnement `TEMP`. Pour examiner la valeur de cette variable, lancez la commande `set`.

Installation à distance

En cas de problèmes avec l'installation à distance, vérifiez les fichiers journaux suivants :

UNIX Serveur d'installation:

`/var/opt/omni/log/IS_install.log`

Client Windows (le système à distance sur lequel les composants doivent être installés) :

- *SystemRoot*`\TEMP\OB2DBG_`*did*`_INSTALL_SERVICE_`*DebugNo*`_debug.txt`
- *SystemRoot*`\TEMP\CLUS_DBG_`*DebugNo*`.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`.

Au cas où les fichiers journaux ne sont pas créés, lancez l'installation à distance avec l'option debug. Voir Création de traces d'exécution d'installation, Page suivante.

Data Protector fichiers journaux

Les fichiers journaux Data Protector listés ci-dessous sont situés dans:

Windows Server 2008 et Windows Server 2012 : *données_programme_Data_Protector*`\log`

Autres systèmes Windows : *répertoire_Data_Protector*`\log`

Systèmes 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`

Les fichiers journaux suivants sont importants pour le dépannage d'installation :

`debug.log`	Contient des conditions inattendues. Tandis que certains peuvent signifier quelque chose pour vous, les informations sont principalement utilisées par l'organisation d'assistance.
`inet.log`	Contient des requêtes faites au service Data Protector `inet`. Ce peut être utile pour vérifier l'activité récente de Data Protector sur les clients.
`IS_ install.log`	Contient une trace d'installation à distance et réside sur le Serveur d'installation.
`omnisv.log`	Contient des informations sur le moment où les services Data Protector ont été arrêtés et démarrés.
`upgrade.log`	Ce journal a été créé au cours de la mise à jour et contient les messages de la partie centrale de la mise à jour (UCP) et de la partie détaillée de la mise à jour (UDP).
`OB2_ Upgrade.log`	Ce journal est créé au cours de la mise à jour et contient des traces du processus de mise à jour.

Pour plus de fichiers journaux, reportez-vous à la section *Guide de dépannage Data Protector*.

Création de traces d'exécution d'installation

Lancez l'installation avec l'option `debug` si cela est demandé par le service d'assistance à la clientèle de. Pour plus d'informations sur le débogage, y compris les options de debug ci-dessous et la préparation des données à envoyer au service d'assistance à la clientèle, reportez-vous à *Guide de dépannage Data Protector*.

Pour une installation du débogage à distance, lancez l'interface graphique utilisateur Data Protector avec l'option de debug :

`Manager -debug 1-200 DebugPostfix`

Une fois la session terminée/abandonnée, collectez la production de debug des emplacements suivants :

- Sur le système Serveur d'installation :

  données_programme_Data_Protector\tmp\OB2DBG_*did*__BM_ *Hostname_DebugNo_ DebugPostfix*
- Sur le système à distance :

  SystemRoot:\Temp\OB2DBG_*did*__INSTALL_SERVICE_*Hostname_DebugNo_DebugPostfix*

Annexe A: Installation et mise à niveau avec les outils d'origine d'un système UNIX

Cette annexe décrit comment installer et mettre à niveau Data Protector sur les systèmes UNIX grâce aux outils d'installation d'origine (`swinstall` sur les systèmes HP-UX et `rpm` sur les systèmes Linux).

Installer sur des systèmes HP-UX et Linux avec des outils natifs

> **REMARQUE :**
> Il est recommandé d'utiliser Data Protector pour installer `omnisetup.sh`. Pour plus d'informations, reportez-vous à Installer sur des systèmes HP-UX et Linux avec des outils natifs, haut.
>
> Utilisez ces procédures d'installation d'origine sur HP-UX et Linux *uniquement* si vous comptez installer un Serveur d'installation avec un nombre limité de packages d'installation distante.

Installer Gestionnaire de cellule sur des systèmes HP-UX avec swinstall

Pour installer un Gestionnaire de cellule UNIX sur un système HP-UX

1. Copiez le package d'installation Data Protector téléchargé (tar) sur le système HP-UX, et extrayez les fichiers vers un répertoire local.
2. Exécutez l'utilitaire `/usr/sbin/swinstall`.
3. Dans la fenêtre Indiquer la source, sélectionnez **Dossier Réseau/CD-ROM**, puis entrez `hpux/DP_DEPOT` dans le **Chemin de Dépôt de la Source**. Cliquez sur **OK** pour ouvrir la fenêtre Installation SD - Sélection du logiciel.
4. Dans la liste des packages disponibles pour l'installation, Data Protector est affiché sous le nom `B6960MA`.
5. Cliquez avec le bouton droit sur **DATA-PROTECTOR**, puis cliquez sur **Marquer pour installer** afin d'installer intégralement le logiciel.

   Si vous n'avez pas besoin de tous les sous-produits, cliquez deux fois sur **DATA-PROTECTOR** puis cliquez avec le bouton droit sur un objet de la liste. Cliquez sur **Ne plus marquer pour installer** pour exclure le package ou sur **Marquer pour installer** pour qu'il soit intégré à l'installation.

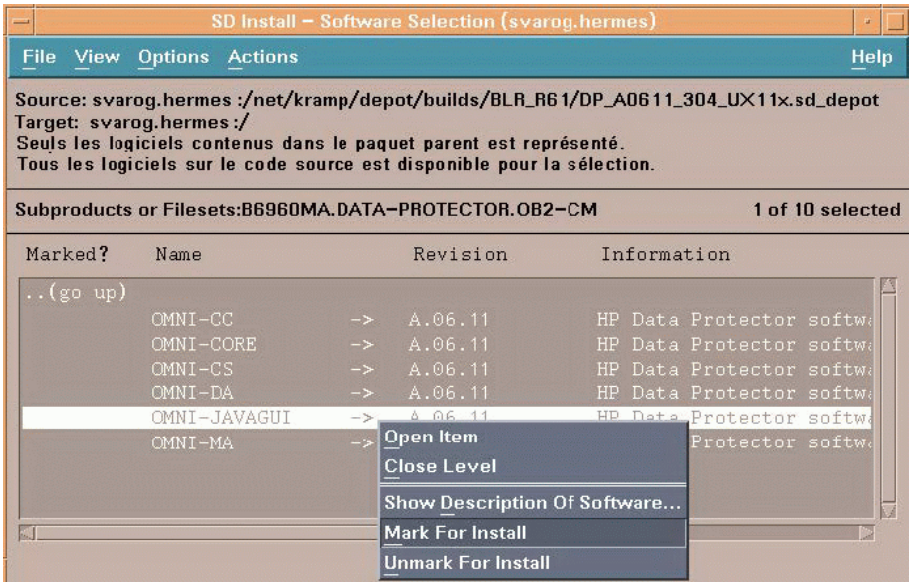
   Les sous-produits suivants sont inclus :

OB2-CM	Logiciel Gestionnaire de cellule
OB2-DOCS	Le sous-produit de documentation Data Protector qui inclut les guides Data Protector au format PDF et le *Aide de Data Protector* au format WebHelp.
OB2-IS	Data Protector pour Serveur d'installation

Assurez-vous que la valeur du statut `Marked?` du package `OB2-CM` soit bien `Yes`si vous installez le Gestionnaire de cellule pour UNIX sur votre système. Voir Fenêtre Installation SD - sélection du logiciel, bas.

> **REMARQUE :**
> Si la longueur des ID utilisateur que vous utilisez est supérieure à 32 bits, vous devez installer à distance le composant Interface Utilisateur (OMNI-CS) sur le Gestionnaire de cellule après avoir installé le composant logiciel Gestionnaire de cellule central.

Fenêtre Installation SD - sélection du logiciel



6. Dans la liste des actions, cliquez sur **Installation (analyse)**, puis cliquez sur **OK** pour valider. Si `Install (analysis)` échoue et affiche un message d'erreur, cliquez sur **Fichier journal** pour voir le fichier.

> **REMARQUE :**
> Pour installer un logiciel depuis un lecteur de bandes situé sur le réseau, vous devez avant tout monter le dossier source sur votre ordinateur.

Installer le Gestionnaire de cellule sur des systèmes Linux avec rpm

Pour installer le Gestionnaire de cellule sur un système Linux

1. Copiez le package d'installation Data Protector téléchargé (tar) sur le système Linux, et extrayez les fichiers vers un répertoire local.
2. Accédez au répertoire `linux_x86_64/DP_DEPOT`.
3. Pour installer un composant, exécutez :

   `rpm -i package_name-A.10.00-1.x86_64.rpm`

   où *nom_du_package* est le nom du package du sous-produit.

Les composants suivants doivent être installés :

OB2-CORE	Client central de Data Protector.
OB2-TS-CORE	Bibliothèques des composants technologiques centraux de Data Protector
OB2-CC	Client de la console de cellule. Contient l'interface en ligne de commande.
OB2-TS-CS	Bibliothèques des composants technologiques de Gestionnaire de cellule.
OB2-TS-JRE	Environnement JRE à utiliser avec Data Protector.
OB2-TS-AS	Serveur d'application de Data Protector
OB2-WS	Services web de Data Protector
OB2-JCE-DISPATCHER	Système de déploiement du moteur de contrôle de tâches
OB2-JCE-SERVICEREGISTRY	Registre de service du moteur de contrôle de tâches
OB2-CS	Client Gestionnaire de cellule.
OB2-DA	Client Agent de disque. Requis, sans quoi il est impossible de sauvegarder l'IDB.
OB2-MA	Client agent général de support Nécessaire pour attacher un périphérique de sauvegarde au Gestionnaire de cellule.
OB2-DOCS	Le sous-produit de documentation Data Protector qui inclut les guides Data Protector au format PDF et le *Aide de Data Protector* au format WebHelp.

IMPORTANT :
Les composants sous Linux sont dépendants les uns des autres. Il est recommandé d'installer les composants dans l'ordre dans lequel ils sont présentés ci-dessus.

4. Redémarrez les services de Data Protector :

```
omnisv stop
omnisv start
```

Installer un Serveur d'installation sur des systèmes HP-UX avec swinstall

1. Copiez le package d'installation Data Protector téléchargé (tar) sur le système HP-UX, et extrayez les fichiers vers un répertoire local.
2. Exécutez l'utilitaire `/usr/sbin/swinstall`.

3. Dans la fenêtre Indiquer la source, sélectionnez **Dossier Réseau/CD-ROM**, puis entrez `hpux/DP_DEPOT` dans le **Chemin de Dépôt de la Source**. Cliquez sur **OK** pour ouvrir la fenêtre Installation SD - Sélection du logiciel.
4. Dans la liste des packages disponibles pour l'installation, Data Protector se trouve sous le nom B6960MA. Cliquez deux fois pour afficher DATA-PROTECTOR pour systèmes UNIX. Cliquez deux fois pour afficher le contenu.

   Les sous-produits suivants sont inclus :

OB2-CM	Logiciel Gestionnaire de cellule
OB2-DOCS	Le sous-produit de documentation Data Protector qui inclut les guides Data Protector au format PDF et le *Aide de Data Protector* au format WebHelp.
OB2-IS	Data Protector pour Serveur d'installation

5. Dans la fenêtre Installation SD - sélection du logiciel, cliquez deux fois sur **DATA-PROTECTOR** pour afficher la liste des logiciels à installer. Cliquez avec le bouton droit sur **OB2-IS**, puis sur **Marquer pour installer**.
6. Depuis le menu Actions, cliquez sur **Installer (analyse)**. Cliquez sur **Suivant** pour valider.

Lorsque l'installation est terminée, le dépôt du logiciel pour UNIX se trouve dans le répertoire `/opt/omni/databases/vendor`.

> **IMPORTANT :**
> Si vous n'installez pas le Serveur d'installation pour UNIX sur votre réseau, il vous faudra installer localement chaque client UNIX avec le package d'installation HP-UX (tar). Qui plus est, il sera impossible de mettre à jour les composants des clients Data Protector.

Installer un Serveur d'installation sur des systèmes Linux avec rpm

Installation locale sur Linux

Pour installer le Serveur d'installation pour UNIX sur un système Linux

1. Copiez le package d'installation Data Protector téléchargé (tar) sur le système Linux, et extrayez les fichiers vers un répertoire local.
2. Accédez au répertoire qui contient l'archive d'installation (dans le cas présent, `linux_x86_64/DP_DEPOT`).
3. Pour chaque composant, exécutez :

   `rpm -i package_name-A.10.00-1.x86_64.rpm`

   Les composants suivants (*nom_du_package*) liés à l'installation du Serveur d'installation sont inclus :

OB2-CORE	Client central de Data Protector. Veuillez noter qu'il est déjà installé si vous installez le Serveur d'installation sur le système du Gestionnaire de cellule.

OB2-TS-CORE	Bibliothèques des composants technologiques centraux de Data Protector.
OB2-CORE-IS	Client central de Serveur d'installation.
OB2-CFP	Client central commun du Serveur d'installation pour toutes les plateformes UNIX.
OB2-TS-CFP	Logiciel commun des composants technologiques du Serveur d'installation pour toutes les plateformes UNIX.
OB2-DAP	Packages d'installation distante de l'agent de disque pour tous les systèmes UNIX.
OB2-MAP	Packages d'installation distante de l'agent de support pour tous les systèmes UNIX.
OB2-NDMPP	Composant de l'agent de support NDMP.
OB2-CCP	Packages d'installation distante de la console de cellule pour tous les systèmes UNIX.

De plus, si vous mettez en place un Serveur d'installation indépendant (c'est à dire qui n'est pas sur le Gestionnaire de cellule) et désirez utiliser l'interface utilisateur :

OB2-CC	Client de la console de cellule. Contient l'interface en ligne de commande.

4. Une fois ces composants installés, utilisez `rpm` pour installer le package d'installation distante pour tous les composants que vous voulez installer à distance. Par exemple :

OB2-INTGP	Client central des intégrations de Data Protector. Ce composant est nécessaire pour installer les intégrations.
OB2-TS-PEGP	Le composant de pile de technologies PEGASUS.
OB2-OR8P	Composant d'intégration Oracle.
OB2-MYSQLP	Composant d'intégration MySQL.
OB2-POSTGRESQLP	Composant d'intégration PostgreSQL.
OB2-SAPP	Composant d'intégration SAP.
OB2-SAPDBP	Composant d'intégration SAP MaxDB.
OB2-SAPHANAP	Composant d'intégration SAP HANA.
OB2-INFP	Composant d'intégration Informix.
OB2-LOTP	Composant d'intégration Lotus Notes/Domino Server.
OB2-SYBP	Composant d'intégration Sybase.
OB2-DB2P	Composant d'intégration DB2.

OB2-EMCP	Composant d'intégration EMC Symmetrix.
OB2-EMCVNXP	Composant d'intégration EMC VNX.
OB2-EMCVMAXP	Composant d'intégration EMC VMAX.
OB2-SMISAP	Composant d'agent P6000 / 3PAR SMI-S.
OB2-SSEAP	Composant d'agent P9000 XP.
OB2-NETAPPP	Composant du fournisseur de stockage NetApp.
OB2-VEPAP	Composant d'agent de protection d'environnement virtuel.
OB2-SODAP	Composant de déduplication du logiciel StoreOnce.
OB2-AUTODRP	Composant de récupération automatique de désastre.
OB2-VMWAREGRE-AGENTP	Composant de l'extension de restauration granulaire VMware.
OB2-DOCSP	Composant de documentation anglaise (Guides, aide).
OB2-FRAP	Composant de documentation française (Guides, aide).
OB2-JPNP	Composant de documentation japonaise (Guides, aide).
OB2-CHSP	Composant de documentation chinoise simplifiée (Guides, aide).

Pour une liste complète des composants et des dépendances, voir Installing a UNIX Gestionnaire de cellule, Page 27:

Lorsque l'installation est terminée, le dépôt du logiciel pour UNIX se trouve dans le répertoire `/opt/omni/databases/vendor`.

IMPORTANT :
Si vous n'installez pas un Serveur d'installation pour UNIX sur votre réseau, il vous faudra installer localement chaque client UNIX avec le package d'installation Linux (tar).

IMPORTANT :
installez Data Protector pour répertoires liés, par exemple :

`/opt/omni/ -> /prefix/opt/omni/`

`/etc/opt/omni/ -> /prefix/etc/opt/omni/`

`/var/opt/omni/ -> /prefix/var/opt/omni/`

vous devez créer les liens avant l'installation et assurer que le répertoire de destination existe.

Étapes suivantes

À ce stade là, les Serveur d'installation pour UNIX devraient être installés sur votre réseau. Il est à présent recommandé d'effectuer les tâches suivantes :

1. Si vous avez mis en place un Serveur d'installation indépendant (c'est à dire, qui n'est pas sur le Gestionnaire de cellule), vous devez ajouter (importer) manuellement le système à la cellule de Data Protector. Voir Installer des Serveur d'installation pour systèmes UNIX, Page 42.

   > **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 pour lister les packages d'installation distante qui ont été installés. Vous pouvez vérifier les packages d'installation distantes disponibles depuis l'interface en ligne de commande. Pour assurer que ce fichier reste à jour, il est recommandé d'exporter et de réimporter un Serveur d'installation à chaque fois que des packages d'installation distante sont installés ou supprimés. Cela s'applique même si un Serveur d'installation est installé sur le même système que le Gestionnaire de cellule.

2. Installez le Serveur d'installation pour Windows au cas où vous auriez un système Windows dans votre cellule Data Protector. Voir Installer sur des systèmes HP-UX et Linux avec des outils natifs, Page 343.
3. Distribuez le logiciel aux clients. Voir Installer des clients Data Protector, Page 54.

Installation des clients

Les clients ne sont pas installés lors de l'installation du Gestionnaire de cellule ou du Serveur d'installation. Les clients doivent être installés avec `omnisetup.sh` ou en installant les composants à distance grâce à l'interface graphique de Data Protector. Pour plus d'informations sur l'installation des clients, reportez-vous à Installer des clients Data Protector, Page 54.

Mise à jour sur les systèmes HP-UX et Linux en utilisant les outils natifs.

Mettre à niveau Data Protector sur des systèmes HP-UX avec swinstall

La mise à niveau d'un Gestionnaire de cellule doit se faire à partir du package d'installation HP-UX.

Si vous mettez à niveau un Gestionnaire de cellule avec un Serveur d'installation installé, vous devez d'abord mettre à niveau le Gestionnaire de cellule puis le Serveur d'installation.

Les composants client installés sur le système du Gestionnaire de cellule ne sont *pas* mis à niveau en même temps que le Gestionnaire de cellule, mais doivent être mis à niveau soit avec `omnisetup.sh`, soit en installant les composants à distance depuis le Serveur d'installation. Pour plus d'informations,

voir Installation locale sur les systèmes UNIX et Mac OS X, Page 103 ou Installation à distance, Page 95.

Procédure de mise à niveau

Pour mettre à niveau vers Data Protector 10.00, avec `swinstall`

1. Exportez l'IDB existante :
   a. Copiez le script `omnimigrate.pl` du package d'installation vers un répertoire temporaire :

      ```
      cp -p MountPoint/hpux/DP_DEPOT/DATA-PROTECTOR/OMNI-CS/opt/omni/sbin/omnimigrate.pl /tmp
      ```

   b. Utilisez la commande `omnimigrate.pl` pour exporter l'IDB :

      ```
      /opt/omni/bin/perl /tmp/omnimigrate.pl -shared_dir /var/opt/omni/server/exported-export
      ```

2. Connectez-vous en tant que `root`et arrêtez les servicesData Protector avec la commande `omnisv -stop`.

   Saisissez `ps -ef | grep omni` pour vérifier que tous les processus ont bien été arrêtés. Il ne doit rester aucun processus Data Protector une fois la commande `ps -ef | grep omni` exécutée.

3. Pour mettre à jour un Gestionnaire de cellule ou/et un Serveur d'installation, suivez les procédures décrites Installer Gestionnaire de cellule sur des systèmes HP-UX avec swinstall, Page 343 ou/et Installer un Serveur d'installation sur des systèmes HP-UX avec swinstall, Page 345.

   La procédure d'installation va automatiquement détecter la version précédente et mettra à niveau *uniquement* les composants sélectionnés. Un composant installé dans la précédente version de Data Protector *n'est pas* mis à niveau s'il n'est pas sélectionné. C'est pourquoi vous devez vous assurer que tous les composants qui doivent être mis à niveau sont sélectionnés.

   > **REMARQUE :**
   > L'option `Match what target has` *n'est pas* prise en charge si vous mettez à niveau le Gestionnaire de cellule et le Serveur d'installation sur le même système.

Mettre à niveau Data Protector sur des systèmes Linux avec rpm

Pour mettre à niveau les versions Linux du Gestionnaire de cellule ou du Serveur d'installation, désinstallez les versions antérieures et installez les nouvelles.

Les composants client installés sur le système du Gestionnaire de cellule ne sont *pas* mis à niveau en même temps que le Gestionnaire de cellule, mais doivent être mis à niveau soit avec `omnisetup.sh`, soit en installant les composants à distance depuis le Serveur d'installation. Pour plus d'informations, voir Installation locale sur les systèmes UNIX et Mac OS X, Page 103 ou Installation à distance, Page 95.

Procédure de mise à niveau

Pour mettre à niveau vers Data Protector 10.00 avec `rpm`

1. a. Copiez le script `omnimigrate.pl` du package d'installation vers un répertoire temporaire :

   ```
   cp –p MountPoint/hpux/DP_DEPOT/DATA-PROTECTOR/OMNI-
   CS/opt/omni/sbin/omnimigrate.pl /tmp
   ```

   b. Utilisez la commande `omnimigrate.pl` pour exporter l'IDB :

   ```
   /opt/omni/bin/perl /tmp/omnimigrate.pl -shared_dir
   /var/opt/omni/server/exported-export
   ```

2. Connectez-vous en tant que `root`et arrêtez les servicesData Protector avec la commande `omnisv -stop`.

   Saisissez `ps -ef | grep omni` pour vérifier que tous les processus ont bien été arrêtés. Il ne doit rester aucun processus Data Protector une fois la commande `ps -ef | grep omni` exécutée.

3. Désinstallez Data Protector à l'aide de`rpm`.

   Les fichiers de configuration et la base de données sont préservées lors de la procédure.

4. Exécutez la commande `rpm –q` pour vérifier que vous avez bien désinstallé la version antérieure de Data Protector. Les versions antérieures de Data Protector ne doivent pas apparaitre dans la liste.

   Vérifiez que la base de données et les fichiers de configuration soient bien présents. Les répertoires suivants doivent toujours exister et contenir les fichiers binaires :

   - `/opt/omni`
   - `/var/opt/omni`
   - `/etc/opt/omni`

5. Si vous mettez un Gestionnaire de cellule à niveau, utilisez `rpm` pour installer le Gestionnaire de cellule. Pour plus d'informations, reportez-vous à la section Installer le Gestionnaire de cellule sur des systèmes Linux avec rpm, Page 344.

   Si vous mettez un Serveur d'installation à niveau, utilisez le package d'installation Linux. Pour plus d'informations, reportez-vous à la section Installer un Serveur d'installation sur des systèmes Linux avec rpm, Page 346.

Annexe B: Préparation du système et maintenance

Cette annexe fournit des informations supplémentaires au sujet de tâches qui sortent du cadre de ce guide mais qui influencent fortement la procédure d'installation. Ces tâches comprennent la préparation du système et la maintenance.

Configuration réseau sur les systèmes UNIX

Quand vous installez Data Protector sur un système UNIX, Data Protector `Inet` est enregistré en tant que service réseau. Cela signifie donc la procédure suivante :

- Modification du `/etc/services` fichier pour enregistrer un port que Data Protector `Inet` va écouter.
- Enregistrement de Data Protector `Inet` Inet dans le daemon `inetd` du système ou son équivalent (`xinetd`, `launchd`).

Quand vous modifiez la configuration d'un réseau, la configuration Data Protector `Inet` Inet initiale peut devenir incomplète ou invalide. Cela arrive chaque fois que vous ajoutez ou retirez des interfaces réseau Internet Protocol version 6 (IPv6) du fait des paramètres spécifiques au système pour ajouter un support IPv6 aux services réseau. Cela peut également arriver en d'autres circonstances.

Pour mettre à jour la configuration Data Protector `Inet` Inet, vous pouvez utiliser l'utilitaire `dpsvcsetup.sh`. Cet utilitaire, aussi utilisé par l'installation et qui rassemble les informations nécessaires et met à jour en conséquence la configuration du système, se trouve dans les répertoires`/opt/omni/sbin` (systèmes HP-UX, Solaris, et Linux) ou `/usr/omni/bin` (autres systèmes UNIX).

- Pour mettre à jour la configuration Data Protector `Inet`, exécutez :

  `dpsvcsetup.sh -update`.
- Pour inscrire Data Protector `Inet` en tant que service réseau, exécutez :

  `dpsvcsetup.sh -install`.
- Pour désinscrire Data Protector `Inet` en tant que service réseau, exécutez :

  `dpsvcsetup.sh -uninstall`.

Vérification de la configuration TCP/IP

La mise en place d'un mécanisme de résolution du nom d'hôte est un élément important du processus de configuration TCP/IP. Chaque système du réseau doit être capable de résoudre l'adresse du Gestionnaire de cellule ainsi que tous les clients avec agents de support et périphériques de support physiques attachés. Le Gestionnaire de cellule doit pouvoir résoudre les noms de tous les clients présents dans la cellule.

Une fois que vous avez installé le protocole TCP/IP, vous pouvez les commandes `ping` et `ipconfig/ifconfig` pour vérifier la configuration TCP/IP.

Notez que sur les systèmes sur lesquels la commande `ping` ne peut pas être utilisée pour les adresses IPv6, la commande `ping6`doit être utilisée.

Pour vérifier la configuration TCP/IP

1. A partir de l'invite des commandes, exécutez :

   Systèmes Windows : `ipconfig /all`

   Systèmes UNIX : `ifconfig`*interface* ou `ifconfig -a` ou `nestat -i`, en fonction du 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 sous-réseau soient correctement définis.
2. Tapez `ping` *votre_adresse_IP* pour confirmer l'installation et la configuration du logiciel. Par défaut, vous devriez recevoir quatre échos de paquets.
3. Tapez `ping` *default_gateway*.

   La passerelle doit se trouver sur votre sous-réseau. Si la commande ping n'aboutit pas, vérifiez si l'adresse IP de la passerelle est correcte et que la passerelle est opérationnelle.
4. Si les étapes précédentes se sont déroulées avec succès, vous êtes prêt à tester la résolution de nom. Indiquez le nom du système dans la commande `ping`pour tester le fichier hosts et/ou le DNS. Si le nom de votre machine était `computer` et le nom de domaine était `company.com`, vous devez entrer : `ping computer.company.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 le processus de résolution de nom pour le système destiné à être le Gestionnaire de cellule et les systèmes destinés à être les clients fonctionne dans les deux sens :

   - Sur le Gestionnaire de cellule, vous pouvez exécuter une commande ping vers chaque client.
   - Sur les clients, vous pouvez exécuter une commande ping vers le Gestionnaire de cellule et chaque client sur lequel est installé un agent de support.

   > **REMARQUE :**
   > Notez que lorsque vous utilisez le fichier hosts pour la résolution de nom, le test ci-dessus ne garantit pas le fonctionnement correct de ce processus. Dans ce cas, vous pouvez utiliser l'**outil de vérification DNS** après l'installation de Data Protector.

   > **IMPORTANT :**
   > Si le processus de résolution de nom expliqué ci-dessus ne fonctionne pas, Data Protector ne peut pas être installé correctement.
   >
   > Notez également que le nom de l'ordinateur Windows doit être identique à celui de l'hôte. Dans le cas contraire, le programme d'installation de Data Protector émet un avertissement.
5. Une fois Data Protector installé et une cellule Data Protector créée, utilisez l'outil de vérification DNS pour vous assurer que le Gestionnaire de cellule et chaque client sur lequel est installé un Agent de support sont en mesure de résoudre correctement les connexions DNS avec tous les autres clients de la cellule, et inversement. Vous pouvez le faire en exécutant la commande `omnicheck -dns` . Les vérifications échouées et le nombre total de vérifications échouées sont affichés.

   Pour plus d'informations sur la commande `omnicheck`, consultez le *Guide de référence de l'interface de ligne de commande Data Protector* .

Changer les ports par défaut de Data Protector

Changer le port Inet par défaut Data Protector

Le service (processus) Data ProtectorInet, qui démarre d'autres processus nécessaires à la sauvegarde et à la restauration, doit utiliser le même port sur chaque système dans la cellule Data Protector.

Par défaut, Inet utilise le numéro de port 5555/5565. Pour vérifier que ce port n'est pas utilisé par un autre programme, vérifiez le fichier /etc/services local (systèmes UNIX) ou la sortie de la commande netstat -a invoquée localement (systèmes Windows). Si le port est déjà utilisé par un autre programme, vous devez reconfigurer Inet pour qu'il utilise un port non utilisé. Cette reconfiguration doit être faite sur *chaque* système de la cellule, afin que *tous* les systèmes dans la cellule utilisent le même port.

Une fois changé sur le Gestionnaire de cellule qui sert aussi de Serveur d'installation, ou sur un Serveur d'installation indépendant, le nouveau port est automatiquement utilisé par tous les clients installés à distance avec ce Serveur d'installation. Le port Inet peut donc être plus facilement modifié lors de la création de la cellule.

> **ATTENTION :**
> Ne modifiez pas le numéro de port d'écoute Inet par défaut préparé pour la récupération après sinistre. Dans le cas contraire, si de tels systèmes sont touchés par un sinistre, le processus de récupération après sinistre pourrait échouer.

Systèmes UNIX

Pour changer le port Inet sur un système UNIX qui deviendra votre client Gestionnaire de cellule, Serveur d'installation, ou Data Protector, procédez comme suit :

- Créez le fichier /tmp/omni_tmp/socket.dat avec le numéro de port souhaité.

Pour changer le port Inet sur un système UNIX qui est déjà votre client Gestionnaire de cellule, Serveur d'installation, ou Data Protector, procédez comme suit :

1. Modifiez le fichier /etc/services. Par défaut, ce fichier doit contenir l'entrée :

   ```
   omni 5565/tcp # DATA-PROTECTOR
   ```

   Remplacez le numéro 5565 par le numéro d'un port non utilisé.
2. Si les fichiers /etc/opt/omni/client/customize/socket et /opt/omni/newconfig/etc/opt/omni/client/customize/socket existent sur le système, actualisez leur contenu avec le numéro de port souhaité.
3. Redémarrez le service Inet en mettant fin au processus concerné à l'aide de la commande kill -HUP *inetd_pid*. Pour déterminer l'ID du processus (*inetd_pid*), utilisez la commande ps -ef.
4. Si vous configurez Inet sur le Gestionnaire de cellule, mettez une nouvelle valeur pour l'option globale Port.
5. Si vous configurez Inet sur le Gestionnaire de cellule, redémarrez les services Data Protector:

```
- omnisv stop
- omnisv start
```

Systèmes Windows

Pour changer le port `Inet` sur un système Windows qui deviendra votre client Gestionnaire de cellule, Serveur d'installation, ou Data Protector

1. Depuis la ligne de commande, lancez `regedit` pour ouvrir l'éditeur de registre.
2. Sous la clé `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Common`, créez l'entrée de registre `InetPort` :

   Nom de l'entrée de registre : `InetPort`

   Type de l'entrée de registre : `REG_SZ (string)`

   Valeur de l'entrée de registre : *PortNumber*

Pour changer le port `Inet` sur un système Windows qui est déjà votre client Gestionnaire de cellule, Serveur d'installation, ou Data Protector

1. Depuis la ligne de commande, lancez `regedit` pour ouvrir l'éditeur de registre.
2. Développez **HKEY_LOCAL_MACHINE**, **SOFTWARE**, **Hewlett-Packard**, **OpenView**, **OmniBack**et sélectionnez **Common**.
3. Cliquez deux fois sur **InetPort** pour ouvrir la boîte de dialogue Modification de la chaîne. Dans la fenêtre de texte Donnée de valeur, entrez le numéro d'un port libre. Recommencez l'opération dans le sous dossier Paramètres du dossier Common.
4. Dans le Panneau de Configuration de Windows, ouvrez **Outils d'administration**, **Services**, puis sélectionnez le service **Data Protector Inet**, et redémarrez-le en cliquant sur l'icône **Redémarrer** de la barre d'outil.

Changer les ports IDB et les comptes utilisateurs par défaut de Data Protector sur des systèmes UNIX

Sur les systèmes UNIX l'installation est faite par le script `omnisetup.sh` et n'est pas interactive. Vous devez changer la valeur des ports dans le fichier `/tmp/omni_tmp/DP.dat` avant de démarrer l'installation.

Les entrées de ports suivantes correspondent aux services IDB :

- Port de service IDB Data Protector HP (hpdp-idb) : PGPORT
- Port du groupeur de connexions IDB Data Protector HP (hpdp-idb-cp) : PGCPORT
- Port de service du serveur d'application Data Protector (hpdp-as) : APPSSPORT
- Port de gestion du serveur d'application Data Protector (hpdp-as) : APPSNATIVEMGTPORT

Vous pouvez changer le compte utilisateur par défaut sous lequel IDB est lancé en modifiant la variable `PGOSUSER`.

Exemple de fichier `DP.dat`:

```
PGPORT=7112
PGCPPORT=7113
PGOSUSER=hpdp
APPSSPORT=7116
APPSNATIVEMGTPORT=7119
```

Préparation d'une grappe de serveurs Microsoft sous Windows Server 2008 ou Windows Server 2012 pour une installation de Data Protector

Pour permettre une installation en grappes de Data Protector sur une grappe de serveurs sous Microsoft Cluster Service (MSCS) de Windows Server 2008 ou de Windows Server 2012, vous devez préparer la grappe à l'avance. Ne pas le faire peut engendrer des erreurs de sessions au moment de sauvegarder l'objet `CONFIGURATION` local, qui doit être sauvegardé pendant la préparation d'un plan de reprise d'activité, et peut même causer une perte de données. Pour plus d'informations sur les combinaisons de rôles de cellules de Data Protector et de versions de système d'exploitation Windows prenant en charge les grappes, consultez les dernières matrices des produits pris en charge sur https://softwaresupport.softwaregrp.com/.

Conditions préalables

- Assurez-vous que vous êtes connecté au système avec le compte utilisateur du domaine. Le compte utilisateur du domaine doit être membre du groupe `Administrators` local.

Procédure de préparation

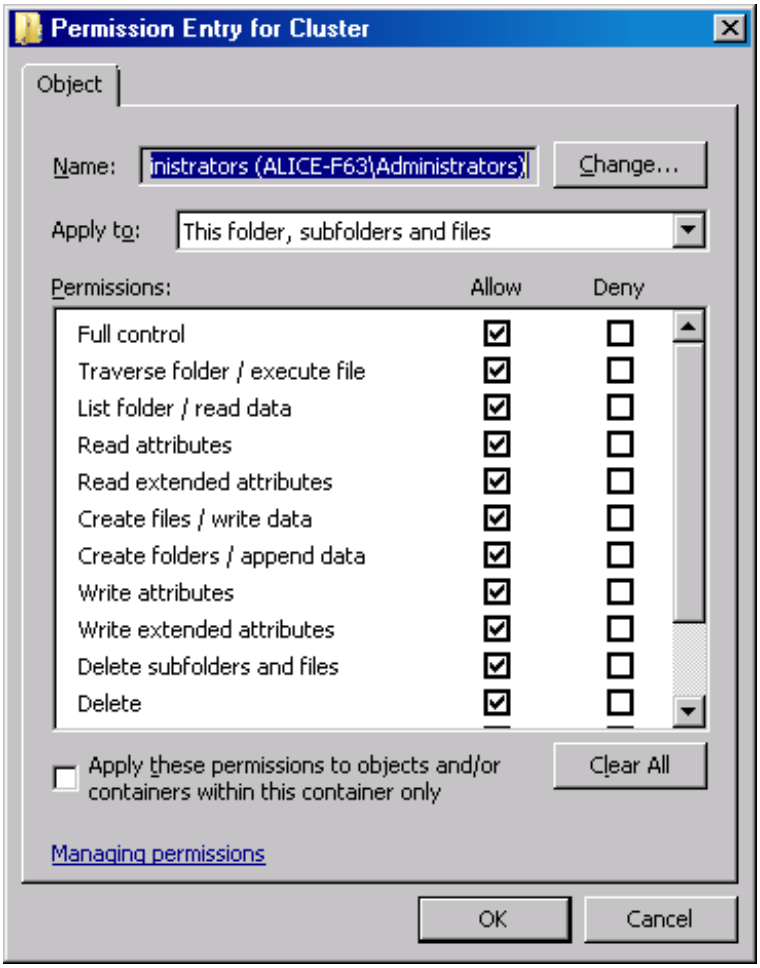
Pour préparer correctement votre cluster pour l'installation de Data Protector, faites ce qui suit :

1. Sur chaque nœud de grappe, lancez le Pare-feu Windows et activez les exceptions pour le logiciel `File and Printer Sharing`.
2. Sur le nœud de grappe actif, lancez la gestion de cluster de basculement et vérifiez que le disque témoin dans la ressource quorum soit en ligne. Si la ressource est hors ligne, passez-la en ligne.

   Effectuez les étapes suivantes uniquement sur le nœud de grappe actif.
3. Si vous préparez un cluster sans avoir configuré un Majority Node Set (MNS), lancez l'explorateur Windows et attribuez la possession du dossier *`WitnessDiskLetter`*`:\Cluster` au groupe `Administrators` local. Pendant que vous changez le propriétaire dans les paramètres de sécurité avancés de la fenêtre du Cluster, assurez-vous que l'option **Remplacer le propriétaire des sous-conteneurs et des objets est cochée**. Dans la boîte de dialogue sécurité de Windows, confirmez l'action suggérée en cliquant sur **Oui**, et confirmez la notification suivante en cliquant à nouveau sur **Oui**.
4. Si vous préparez un cluster sans avoir configuré un MNS, dans l'explorateur Windows, changez la possession du dossier *`WitnessDiskLetter`*`:\Cluster` pour permettre un contrôle total au groupe `SYSTEM` et au groupe `Administrators` local. Vérifiez que les paramètres d'autorisation pour les

deux groupes correspondent à ceux affichés dans Permissions pour le dossier Cluster et pour le groupe utilisateur Administrateurs local, bas.

Permissions pour le dossier Cluster et pour le groupe utilisateur Administrateurs local



5. Si vous préparez un cluster pour qu'il prenne le rôle de gestionnaire de cellule Data Protector, ajoutez une ressource `Cluster Access Point` dans le gestionnaire de cluster de basculement. Sélectionnez **Ajouter une ressource** et cliquez sur **1- Point d'accès client** pour lancer l'assistant Nouvelle ressource :
   a. Sur le panneau Point d'accès client, entrez le nom du réseau du serveur virtuel dans le champ prévu pour le nom.
   b. Entrez l'adresse IP du serveur virtuel dans le champ prévu pour l'adresse.
6. Si vous préparez un cluster pour qu'il prenne le rôle de gestionnaire de cellule Data Protector, ajoutez un dossier partagé au cluster dans le gestionnaire de cluster de basculement. Lancez l'assistant Prévision d'un dossier partagé en cliquant sur **Ajouter un dossier partagé** :
   a. Sur le panneau localisation du dossier partagé, entrez le chemin du répertoire dans le champs prévu pour le répertoire. Assurez-vous que le répertoire choisi dispose d'assez d'espace libre pour recevoir les données créées lors de l'installation de Data Protector. Cliquez sur **Suivant**.
   b. Sur les panneaux Permissions NTFS, Protocoles partagés et Paramètres SMB, laissez les valeurs des options par défaut inchangées. Cliquez sur **Suivant** pour passer au panneau

suivant.

c. Sur le panneau des Permissions SMB, sélectionnez l'option **Les Administrateurs ont le contrôle total; tous les autres utilisateurs et groupes disposent seulement des accès Lire et Écrire**. Cliquez sur **Suivant**.

d. Sur l'écran des espaces de noms DFS, laissez les valeurs par défaut des options. Cliquez sur **Suivant**.

e. Sur le panneau Vérifier 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, suivez d'abord la procédure générale pour l'installation de Data Protector sur MSCS. Voir Installation de Data Protector sur Microsoft Cluster Server, Page 180.

Une fois l'installation terminée, quelques manipulations supplémentaires sont nécessaires pour activer le service `Data Protector Inet` afin de différencier les ressources locales des ressources de disque cluster qui utilisent leur propre pilote de ressources et non le pilote de ressources de Microsoft :

1. Démarrez le mode maintenance en exécutant la commande `omnisv -maintenance` sur le Gestionnaire de cellule.
2. Définissez une nouvelle variable d'environnement système `OB2CLUSTERDISKTYPES` avec `Volume Manager Disk Group` comme valeur, ou mettez l'option `omnirc`sur les deux nœuds de grappe comme indiqué :

   ```
   OB2CLUSTERDISKTYPES=Volume Manager Disk Group
   ```

   Pour spécifier des ressources disque propriétaires supplémentaires, comme NetRAID4 disk, ajoutez simplement le nom du type de 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 options du fichier `omnirc`, reportez-vous au *Guide de dépannage Data Protector*.
3. Quittez le mode maintenance en exécutant la commande `omnisv -maintenance –stop`

Préparation d'un serveur NIS

Cette procédure permet à votre serveur NIS de reconnaître votre Data ProtectorGestionnaire de cellule.

Pour ajouter l'information Data Protector à votre serveur NIS

1. Connectez-vous en tant que `root`sur le serveur `NIS`.
2. Si vous gérez le fichier `/etc/services` via `NIS`, ajoutez la ligne suivante au fichier `/etc/services`:

   ```
   omni 5565/tcp # Data Protector for Data Protector inet server
   ```

Remplacez 5565 si le port n'est pas disponible. Voir Changer le port Inet par défaut Data Protector, Page 354.

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. Lancez la commande suivante pour que le serveur `NIS`puisse lire le fichier et mettre à jour la configuration.

```
cd /var/yp; make
```

> **REMARQUE :**
> Dans l'environnement `NIS`, le fichier `nsswitch.conf`définit l'ordre d'utilisation des différentes configurations. Par exemple, vous pouvez définir si le fichier `/etc/inetd.conf` sera utilisé sur la machine locale ou depuis le serveur `NIS`. Vous pouvez également insérer une phrase dans le fichier pour indiquer que le fichier `nsswitch.conf` contrôle l'emplacement où sont conservés les noms. Reportez-vous au manuel pour plus d'informations.
>
> Si vous avez déjà installé Data Protector, vous devez préparer le serveur `NIS`, puis redémarrer le service `inet`en tuant le processus concerné grâce à la commande `kill -HUP` *`pid`* sur chaque client `NIS`servant également de client Data Protector.

Dépannage

- Si le service `Data Protector Inet` Inet ne démarre pas une fois Data Protector installé sur votre environnement NIS, vérifiez le fichier `/etc/nsswitch.conf` .

  Si vous trouvez la ligne suivante :

  ```
  services: nis [NOTFOUND=RETURN] files
  ```

  remplacez la ligne par :

  ```
  services: nis [NOTFOUND=CONTINUE] files
  ```

Modification du nom du Gestionnaire de cellule

Quand Data Protector est installé, il donne au Gestionnaire de cellule le même nom que le nom d'hôte actuel. Si vous changez le nom d'hôte de votre Gestionnaire de cellule, vous devrez mettre à jour les fichiers Data Protector manuellement.

> **IMPORTANT :**
> Il est nécessaire de mettre à jour les informations client qui concernent le nom du Gestionnaire de cellule. Avant de changer le nom d'hôte de votre Gestionnaire de cellule, exportez les clients de la cellule. Pour connaître la procédure, voir Exportation de clients d'une cellule, Page 198. Une fois le nom d'hôte changé, importez à nouveau les clients dans la cellule.

> **REMARQUE :**
> Les périphériques et spécifications de sauvegarde configurés en utilisant le nom antérieur du Gestionnaire de cellule doivent être modifiés pour correspondre au nouveau nom.

Sur les systèmes UNIX

Pour un Gestionnaire de cellule UNIX, procédez comme suit :

1. Modification du nom d'ordinateur ou de domaine.

   > **REMARQUE :**
   > Assurez-vous que le nouveau nom d'hôte est résolu via le DNS sur tous les membres et dans les deux directions. Ne poursuivez pas cette procédure si la résolution du nom ne fonctionne pas.

2. Exécutez la commande suivante :

   ```
   omnisv stop
   ```

   > **REMARQUE :**
   > Assurez-vous qu'aucune instance de l'ancien nom d'hôte n'existe dans le fichier suivant :
   >
   > `/etc/opt/omni/client/components`

   Vous pouvez exécuter la commande suivante :

   ```
   "grep -rn /etc/opt/omni/client/components -e "<OLD_HOSTNAME_FQDN>""
   ```

3. Changez les entrées de 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/config
   /etc/opt/omni/server/cell/installation_servers
   /etc/opt/omni/server/users/UserList
   ```

4. Générez à nouveau le certificat en exécutant la commande suivante :

   ```
   # perl -CA /opt/omni/sbin/omnigencert.pl -server_id <NEW_HOSTNAME_FQDN> -
   server_san dns:<short_hostname>,dns:< NEW_HOSTNAME_FQDN > -user_id hpdp -store_
   password <STORE_PASSWORD>
   ```

   > **REMARQUE :**
   > Vous trouverez keystorepassword en exécutant la commande suivante :
   >
   > `# grep keystorePassword`
   >
   > `/etc/opt/omni/client/components/webservice.properties`

5. Exécutez la commande suivante :

   ```
   omnisv start
   ```

6. Changez le nom du Gestionnaire de cellule dans l'IDB en utilisant la commande :

   ```
   omnidbutil -change_cell_name
   ```

7. Connectez-vous au Gestionnaire de cellule en utilisant l'interface graphique de Data Protector et acceptez le nouveau certificat
8. Si un périphérique à bandes est connecté au Gestionnaire de cellule, naviguez vers **Périphériques et supports**, et modifiez le nom d'hôte dans les propriétés du périphérique à bandes.

9. Dans le cas d'un périphérique de fichiers configuré :
   a. Pour afficher les périphériques configurés, utilisez les instructions suivantes :

      "omnidownload -list_libraries [-detail]" and "omnidownload -dev_info"

   b. Pour modifier le nom d'hôte dans la bibliothèque, accédez à `# omnidownload -library <LIBRARY_NAME> >/tmp/file_lib.txt` et éditez le fichier `file_lib.txt` comme suit :

      `# omniupload -modify_library <LIBRARY_NAME> -file /tmp/file_lib.txt`

   c. Pour modifier le nom d'hôte dans la liste des périphériques, accédez à `# omnidownload -device <DRIVE_NAME> >/tmp/writer_0.txt` et éditez le fichier `writer_0.txt` comme suit :

      `# omniupload -modify_device <DRIVE_NAME> -file /tmp/writer_0.txt`

10. Supprimez la spécification de sauvegarde dans la base IDB Data Protector et recréez-en une nouvelle.
11. Modifiez les autres spécifications de sauvegarde concernées par le changement du nom d'hôte.
12. Mettez à jour les clients UNIX ou LINUX pour refléter le changement de nom d'hôte du serveur de cellule dans les situations suivantes :

    `/etc/opt/omni/client/cell_server`

13. Mettez à jour les clients Windows pour refléter le changement de nom d'hôte du serveur de cellule dans le registre :

    `HKEY_LOCAL_MACHINE -> SOFTWARE -> Hewlett Packard -> OpenView -> OmniBack II -> Site -> CellServer`

14. Vérifiez le fichier de configuration de l'ancien nom d'hôte :

    `# grep -rn /etc/opt/omni -e "<OLD_HOSTNAME_FQDN>"`

    > **REMARQUE :**
    > Il est acceptable de visualiser l'ancien nom d'hôte aux emplacements suivants :
    >
    > `/etc/opt/omni/server/dr/p1s -> If the system recovery data has been stored in the past.`
    >
    > `/etc/opt/omni/server/certificates -> old certificate`
    >
    > `/etc/opt/omni/client/certificates -> old certificate`

15. Vérifiez le contenu de l'ID et exportez-le vers le fichier suivant :

    `/opt/omni/sbin/omnidbutil -writedb /tmp`

    `<ENTER>`

    > **REMARQUE :**
    > Le fichier `dpidb.dat` contient la majeure partie de la base de données interne. Les tables dans lesquelles l'ancien nom d'hôte peut subsister sont les suivantes :
    >
    > `dp_frontend_application`
    >
    > `dp_catalog_object`
    >
    > `dp_catalog_object_datastream (in case the old device name(s) contain the old hostname)`
    >
    > `dp_management_session`
    >
    > `dp_medmng_library (in case the current device name(s) contain the old hostname)`

```
dp_medmng_media_pool (in case the old pool name(s) contain the old
hostname)
dp_medmng_cartridge (in case the old pool name(s) contain the old
hostname)
```

De même, le fichier `dpjce.dat` contient la base de données JCE (Job Control Engine). Son contenu inclut quelques entrées d'URL indispensables pour le planificateur. L'ancien nom d'hôte ne doit pas exister dans ce fichier

Si vous trouvez l'ancien nom d'hôte dans la table `jce_service_description`, procédez comme suit :

a. Connectez-vous à la base de données hpjce.

> **REMARQUE :**
> Vous trouverez les informations d'identification à la base de données dans le fichier `/etc/opt/omni/server/idb/idb.config` fichier

```
# grep PGSUPERPASSWORD /etc/opt/omni/server/idb/idb.config
PGSUPERPASSWORD='a2ZudGV4cjBpdTZnMg==';
# export PGPASSWORD=`echo 'a2ZudGV4cjBpdTZnMg==' | base64 -d`
# echo $PGPASSWORD
kfntexr0iu6g2
```

b. Créez une connexion. Procédez comme suit :

i. Dans une invite de commande, naviguez vers `bin` (`/opt/omni/idb/bin/`).

ii. Exécutez la commande suivante pour vous connecter à la base de données hpjce avec l'identité de l'utilisateur hpdp :

```
# /opt/omni/idb/bin/psql -h localhost -p 7112 -U hpdp hpdpidb
psql (9.1.9)
Type "help" for help.
```

iii. Vérifiez le contenu actuel en exécutant la commande suivante sur la base de données hpjce :

```
hpjce=# select url from jce_service_description;
```

> **REMARQUE :**
> Si vous devez modifier le nom d'hôte, exécutez les commandes suivantes :
>
> ```
> hpjce=# update jce_service_description
> hpjce-# set url=replace(url, 'old_hostname', 'new_hostname');
> hpjce=# \q
> ```

Sur les systèmes Windows

Pour un Gestionnaire de cellule Windows, procédez comme suit :

1. Modification du nom d'ordinateur ou de domaine.

   > **REMARQUE :**
   > Assurez-vous que le nouveau nom d'hôte est résolu via le DNS sur tous les membres et dans les deux directions. Ne poursuivez pas cette procédure si la résolution du nom ne fonctionne pas.

2. Exécutez la commande suivante :

   ```
   omnisv stop
   ```

3. Changez le nom du Gestionnaire de cellule dans la clé de registre suivante :

   ```
   HKEY_LOCAL_
   MACHINE\SOFTWARE\HewlettPackard\OpenView\OmniBackII\Site\CellServer\newnameHKE
   Y_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Packages\newname
   ```

4. Naviguez vers le fichier suivant pour vous assurer qu'aucune instance de l'ancien nom d'hôte n'existe encore :

   ```
   Data_Protector_program_data\Config\client\components
   ```

   > **REMARQUE :**
   > Utilisez la fonction `find in file` de Windows.

5. Changez les entrées de nom d'hôte du Gestionnaire de cellule dans les fichiers suivants :

   données_programme_Data_Protector\Config\Server\users\UserList

   données_programme_Data_Protector\Config\Server\config

   données_programme_Data_Protector\Config\Server\cell\cell_info

   données_programme_Data_Protector\Config\Server\cell\installation_servers

6. Générez à nouveau le certificat en exécutant la commande suivante à partir du dossier `C:\Program Files\OmniBack\bin`:

   ```
   perl omnigencert.pl -server_id <NEW_HOSTNAME> -server_san
   dns:<hostname>,dns:<FQDN> -user_id hpdp -store_password <PASSWORD>
   ```

   > **REMARQUE :**
   > Vous trouverez keystorepassword à l'emplacement suivant.
   >
   > *données_programme_Data_*
   > *Protector*\Config\client\components\webservice.properties

7. Exécutez la commande suivante :

   ```
   omnisv start
   ```

8. Changez le nom du Gestionnaire de cellule dans l'IDB en utilisant la commande :

   ```
   omnidbutil -change_cell_name
   ```

9. Connectez-vous au Gestionnaire de cellule en utilisant l'interface graphique de Data Protector et acceptez le nouveau certificat.
10. Si un périphérique à bandes est connecté au Gestionnaire de cellule, naviguez vers **Périphériques et supports**, et modifiez le nom d'hôte dans les propriétés du périphérique à bandes.
11. Dans le cas d'un périphérique de fichiers configuré :

a. Pour afficher les périphériques configurés, utilisez les instructions suivantes :

   "omnidownload -list_libraries [-detail]" and "omnidownload -dev_info"

b. Pour modifier le nom d'hôte dans la bibliothèque, accédez à "omnidownload -library <LIBRARY_NAME> > c:\temp\file_lib.txt" et éditez le fichier file_lib.txt comme suit :

   omniupload -modify_library <LIBRARY_NAME> -file c:\temp\file_lib.txt

c. Pour modifier le nom d'hôte dans la liste des périphériques, accédez à "omnidownload -device <Device Name> > c:\temp\device.txt" et éditez le fichier device.txt comme suit :

   omniupload -modify_device <Device Name> -file c:\temp\device.txt

12. Supprimez la spécification de sauvegarde dans la base IDB Data Protector et recréez-en une nouvelle.
13. Modifiez les autres spécifications de sauvegarde concernées par le changement du nom d'hôte.
14. Mettez à jour les clients UNIX ou LINUX pour refléter le changement de nom d'hôte du serveur de cellule dans les situations suivantes :

    /etc/opt/omni/client/cell_server

15. Mettez à jour les clients Windows pour refléter le changement de nom d'hôte du serveur de cellule dans le registre :

    HKEY_LOCAL_MACHINE -> SOFTWARE -> Hewlett Packard -> OpenView -> OmniBack II -> Site -> CellServer

16. Vérifiez le fichier de configuration suivant avec la fonction "find in file" de Windows pour trouver l'ancien nom d'hôte :

    données_programme_Data_Protector\Config

    > **REMARQUE :**
    > Il est acceptable de visualiser l'ancien nom d'hôte aux emplacements suivants :
    >
    > *données_programme_Data_Protector*\Config\Server\dr -> Si la récupération du système a été stockée dans le passé.
    >
    > *données_programme_Data_Protector*\Config\Server\certificates -> old certificate
    >
    > *données_programme_Data_Protector*\Config\client\certificates -> old certificate

17. Vérifiez le contenu de l'ID et exportez-le vers le fichier suivant :

    omnidbutil -writedb e:\idb_export

    <ENTER>

    > **REMARQUE :**
    > Le fichier dpidb.dat contient la majeure partie de la base de données interne. Les tables dans lesquelles l'ancien nom d'hôte peut subsister sont les suivantes :
    >
    > dp_frontend_application
    >
    > dp_catalog_object
    >
    > dp_catalog_object_datastream (in case the old device name(s) contain the old hostname)
    >
    > dp_management_session

```
dp_medmng_library (in case the current device name(s) contain the old
hostname)
dp_medmng_media_pool (in case the old pool name(s) contain the old
hostname)
dp_medmng_cartridge (in case the old pool name(s) contain the old
hostname)
```

De même, le fichier `dpjce.dat` contient la base de données JCE (Job Control Engine). Son contenu inclut quelques entrées d'URL indispensables pour le planificateur. L'ancien nom d'hôte ne doit pas exister dans ce fichier.

Si vous trouvez l'ancien nom d'hôte dans la table `jce_service_description`, procédez comme suit :

a. Connectez-vous à la base de données hpjce.

> **REMARQUE :**
> Vous trouverez les informations d'identification à la base de données dans le fichier *données_programme_Data_Protector*`\Config\Server\idb\idb.config`. Vous pouvez utiliser le lien suivant pour décoder `PGSUPERPASSWORD` :
>
> https://www.base64decode.org

b. Créez une connexion. Procédez comme suit :

   i. Dans une invite de commande, naviguez vers `bin` (`C:\Program Files\OmniBack\idb\bin`).

   ii. Exécutez la commande suivante pour vous connecter à la base de données hpjce avec l'identité de l'utilisateur hpdp :

   ```
   .\psql -h localhost -p 7112 -d hpjce -U hpdp <Enter the decoded
   password>
   ```

   iii. Vérifiez le contenu actuel en exécutant la commande suivante sur la base de données hpjce :

   ```
   hpjce=# select url from jce_service_description;
   ```

   > **REMARQUE :**
   > Si vous devez modifier le nom d'hôte, exécutez les commandes suivantes :
   >
   > ```
   > hpjce=# update jce_service_description
   > hpjce-# set url=replace(url, 'old_hostname', 'new_hostname');
   > hpjce=# \q
   > ```

Modification du nom d'hôte dans la base de données JCE (Job Control Engine)

Sur les systèmes UNIX

Pour modifier le nom d'hôte dans une base de données JCD avec PGADMIN3, procédez comme suit :

1. Naviguez vers le fichier `/var/opt/omni/server/db80/pg/pg_hba.conf`.
2. Remplacez `host all all 127..0.0.1/32 md5` par `host all all 10.17.0.0/16 md5`.

   (OU)

   Modifiez `host all all 127..0.0.1/32 md5` pour vous connecter à un hôte spécifique (`host all all 10.17.16.121/32 md5`) uniquement.
3. Rechargez le fichier `pg config` et exécutez les commandes suivantes :

   ```
   su hpdp
   /opt/omni/idb/bin/pg_ctl reload -D /var/opt/omni/server/db80/pg
   ```
4. Connectez-vous à pgAdmin3.

Sur les systèmes Windows

Pour modifier le nom d'hôte dans une base de données JCD en utilisant la ligne de commande avec PGADMIN3, procédez comme suit :

1. Exécutez la commande suivante :

   ```
   omnidbutil –set_passwd hpdp
   ```
2. Définissez le mot de passe.
3. Naviguez vers le dossier `C:\Program Files\OmniBack\idb\bin` et exécutez **pgadmin3.exe**.

   Le programme pgAdmin3 est lancé.
4. Ajoutez le serveur en cliquant sur le plug-in  .

   La fenêtre Enregistrement d'un nouveau serveur s'affiche.
5. Dans la fenêtre Enregistrement d'un nouveau serveur, effectuez ce qui suit :
   a. Dans le champ Nom, saisissez local ou la valeur souhaitée.

      Vous pouvez entrer jce_service_description à titre d'exemple.
   b. Dans le champ Hôte, saisissez localhost.
   c. Dans le champ Port, saisissez 7112.
   d. Dans le champ Service, ne saisissez rien.
   e. Dans le champ Base de données de maintenance, sélectionnez hpdpidb.
   f. Dans le champ Nom d'utilisateur, saisissez hpdp.
   g. Dans le champ Mot de passe, saisissez le mot de passe que vous avez défini avec la commande `omnidbutil –set_passwd hpdp` à l'Étape 1.
6. Cliquez sur **OK**.
7. Dans la zone de navigateur Objet, développez le serveur que vous avez ajouté en développant Bases de données > hpjce > Schémas > hpjce_app > Tables.

   Par exemple : Vous pouvez voir le nom de table `jce_service_description`. Cliquez sur jce_service_description.
8. Sélectionnez le bouton SQL dans la barre d'outils.

   Vous pouvez afficher l'éditeur SQL avec la commande suivante :

   ```
   UPDATE jce_service_description
   ```

```
SET url=replace (url, ‘old_hostname’, ‘new_hostname’);
```

Par exemple, vous pouvez utiliser `testHostname.1` pour old_hostname et `testHostname` pour new_hostname. Exécutez ensuite cette commande avec le bouton Lire.

Dans l'onglet Sortie de données, vous pouvez voir le message indiquant le nombre de lignes modifiées.

Utilisation de la ligne de commande

Pour modifier le nom d'hôte dans une base de données JCD sans PGADMIN3, procédez comme suit :

1. Exécutez ce qui suit :

   Sur un système Windows :

   ```
   C:\Program Files\OmniBack\idb\psql --port=7112 -U hpdp -d hpjce -h localhost
   ```

   Sur un système UNIX :

   ```
   /opt/omni/idb/bin/psql --port=7112 -U hpdp -d hpjce -h localhost
   ```

2. Exécutez les commandes suivantes :

   ```
   hpjce=# select url from jce_service_description;
   hpjce=# update jce_service_description
   hpjce-# set url=replace(url, 'old_hostname', 'new_hostname');
   hpjce=# \q
   ```

Exécution de sessions de sauvegarde massive sous Windows Gestionnaire de cellule

Pour exécuter un grand nombre de sessions de sauvegarde sur Gestionnaire de cellule, vous devez ajuster la limite d'accumulation du bureau dans le registre Windows. L'accumulation du bureau est contrôlée par la clé de registre suivante :

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

La valeur par défaut de cette clé de registre est la suivante :

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

Data Protector est affecté par le paramètre `SharedSection` qui comprend les valeurs suivantes :

- `1024`Taille de l'accumulation partagée commune à tous les bureaux. Elle ne doit pas être changée pour répondre à des problèmes liés à l'épuisement de l'accumulation du bureau.
- `20480`: Taille de l'accumulation du bureau pour chaque bureau associé à un poste de fenêtre interactif.
- `768`: Taille de l'accumulation du bureau pour chaque bureau associé à un poste de fenêtre non-interactif.

Vous devez définir la troisième valeur (`768`) du paramètre `SharedSection` pour `20480`. La valeur modifiée de la clé du registre Windows ressemblera à ce qui suit :

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

> **REMARQUE :**
> Ne définissez pas une valeur très haute, comme c'est le cas dans les kilobites.

Après avoir défini la nouvelle valeur, vous devez redémarrer le système.

Annexe C: Tâches liées aux périphériques et aux supports

Cette annexe fournit des informations supplémentaires spécifiques à Data Protector au sujet de tâches non concernées par ce guide. Ces tâches comprennent la configuration des pilotes de périphériques, la gestion de robots SCSI, la maintenance d'un environnement SCSI, et tout ce qui s'y apparente.

Utilisation de lecteurs bande et robotique sur systèmes Windows

Data Protector prend en charge les pilotes de bandes d'origine qui sont chargés par défaut pour tout lecteur de bande attaché à un système Windows. Les pilotes Windows d'origine chargés pour les changeurs de média (robots) ne sont pas pris en charge par Data Protector.

Dans les exemples ci-dessous, un périphérique à bande 4mm DDS est attaché au système Windows. Le pilote d'origine chargé pour le changeur de média doit être désactivé si le périphérique à bande 4mm DDS est connecté au système Windows et doit être configuré pour être utilisé avec Data Protector. Cette section décrit les procédures qui y sont liées.

Pilotes de bandes

Un pilote est normalement fourni avec Windows, si le périphérique se trouve dans la Hardware Compatibility List (HCL). HCL est une liste de périphériques pris en charge par Windows qui peut être trouvée sur la page suivante :

http://www.microsoft.com/whdc/hcl/default.mspx

Les drivers sont automatiquement chargés pour tous les périphériques approuvés au démarrage de l'ordinateur. Vous n'avez pas besoin de charger séparément un pilote de bandes d'origine, mais vous pouvez le mettre à jour.

Pour mettre à jour ou remplacer un pilote de bandes d'origine sur un système Windows.

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. Étendez les périphériques à bande. Pour vérifier quel pilote est actuellement chargé sur le périphérique, cliquez avec le bouton droit sur le périphérique à bande puis sur **Propriétés**.
4. Sélectionnez l'onglet **Pilote** et cliquez sur **Mettre à jour le pilote**. Suivez les instructions de l'assistant qui vous permettra de spécifier si vous voulez mettre à jour le pilote de bandes d'orgine actuellement installé ou le remplacer par un différent.
5. Redémarrez le système pour appliquer les changements.

> **IMPORTANT :**
> Si un périphérique a déjà été configuré pour Data Protector sans utiliser de pilote de bandes d'origine,

vous devez renommer les fichiers du périphérique pour tous les périphériques de sauvegarde de Data Protector configurés qui font référence à ce lecteur de bandes en particulier (par exemple, de `scsi1:0:4:0` en `tape3:0:4:0`).

Pour plus d'informations, voir Créer des fichiers de périphérique (adresses SCSI) sur des systèmes Windows, Page 372.

Pilotes de robots

Sous Windows, les pilotes de robots sont automatiquement chargés pour activer les librairies de sauvegarde.. Pour utiliser les robots de librairie avec Data Protector, vous devez désactiver le pilote correspondant.

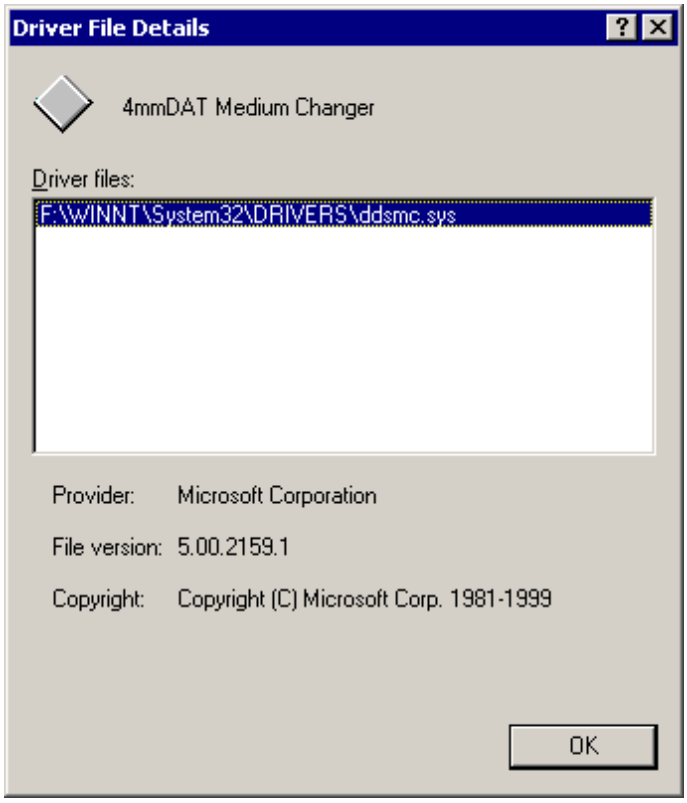
Une librairie de sauvegarde 1557A avec bandes 4mm DDS est utilisée dans l'exemple ci-dessous.

Pour désactiver le pilote de robots (`ddsmc.sys`) chargé automatiquement sur un système Windows

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 du Gestionnaire de périphériques, développez Changeur de média.
4. Pour vérifier quel pilote est actuellement chargé, cliquez avec le bouton droit sur **Changeur de média 4mm DDS** puis sur **Propriétés**.

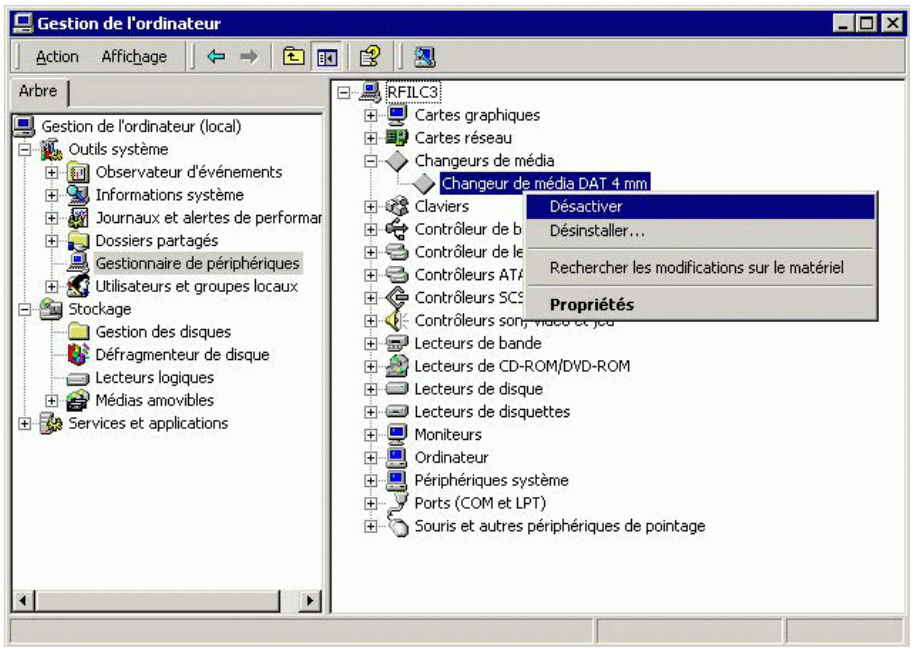
   Sélectionnez l'onglet **Pilote** et cliquez sur **Détails du pilote**. Dans le cas présent, la fenêtre suivante sera affichée :

   Propriétés du Changeur de média



Pour désactiver le pilote de robots d'origine, cliquez avec le bouton droit sur **Changeur de média 4mm DDS** puis sélectionnez **Désactiver**.

Désactiver les pilotes de robots



5. Redémarrez le système pour appliquer les changements. Les robots peuvent maintenant être configurés avec Data Protector.

Créer des fichiers de périphérique (adresses SCSI) sur des systèmes Windows

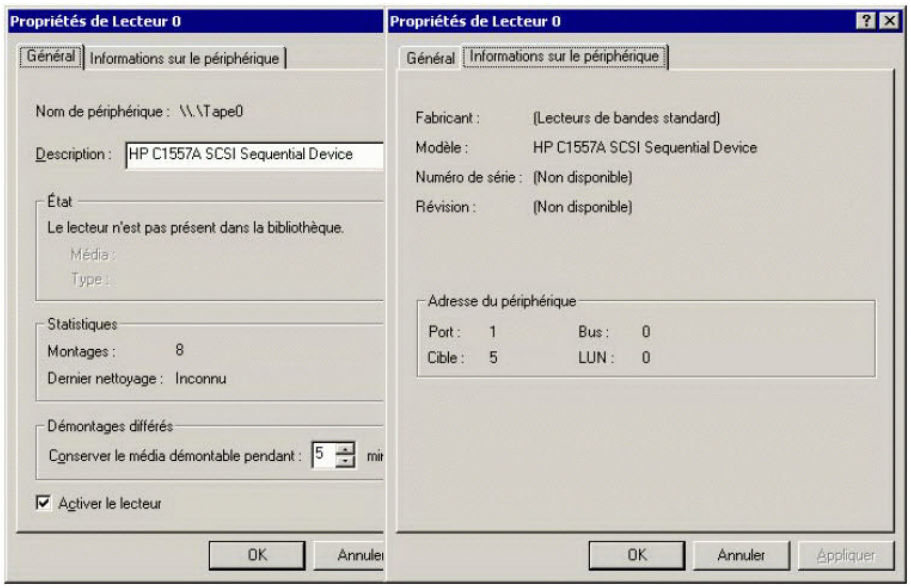
La syntaxe du nom de fichier du lecteur de bande dépend de si le pilote de bandes d'origine a été chargé `tapeN:B:T:L` ou non `scsiP:B:T:L` pour le lecteur de bande.

Windows avec pilote de bandes d'origine

Pour créer un fichier de périphérique pour un lecteur de bande connecté à un système Windows qui utilise le pilote de bandes d'origine, 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 sur le lecteur de bande avec le bouton droit de la souris, 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 trouverez les informations nécessaires dans la page des propriétés Informations sur le périphérique. Voir Propriétés d'un lecteur de bande, bas.

Propriétés d'un lecteur de bande



Le nom de fichier trouvé dans Propriétés d'un lecteur de bande, haut est créé comme suit :

Pilote de bandes d'origine utilisé	`Tape0 or Tape0:0:5:0`
Pilote de bandes d'origine NON utilisé	`scsii1:0:5:0`

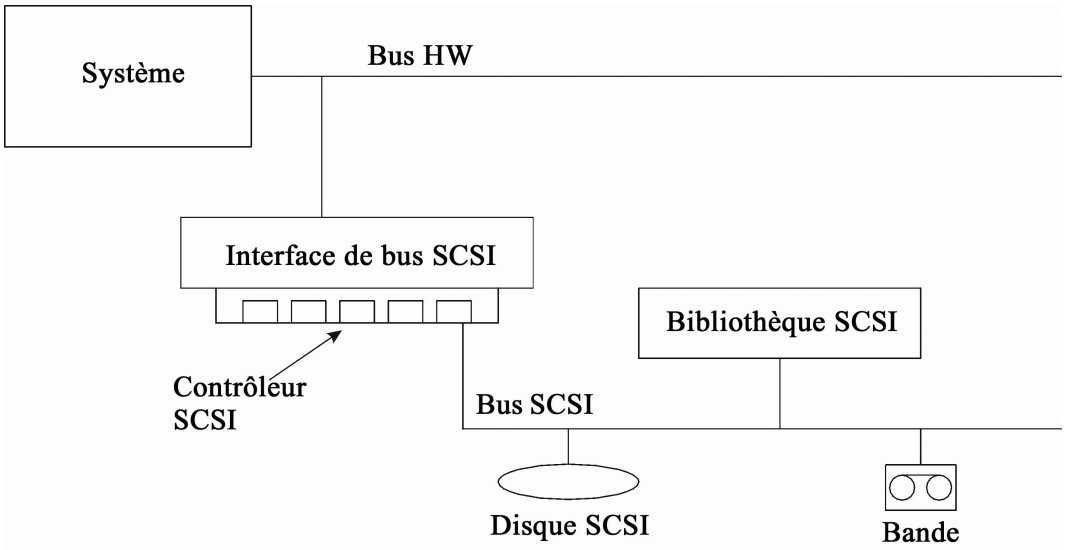
Périphériques magnéto-optique

Si vous connectez un périphérique magnéto-optique à un système Windows, une lettre de périphérique lui est assignée après redémarrage du système. Cette lettre de périphérique est alors utilisée quand vous créez le fichier de périphérique. Par exemple, `E:` est le fichier de périphérique créé pour un périphérique magnéto-optique auquel la lettre `E` a été assignée.

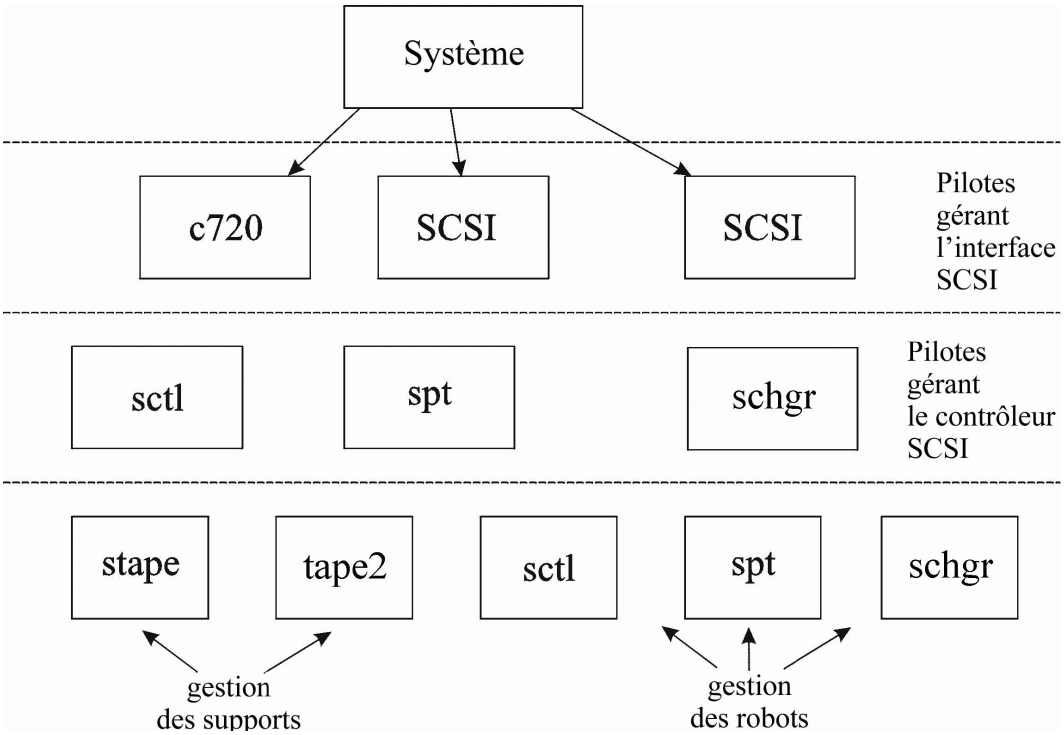
Configuration de robotiques SCSI sur systèmes HP-UX

Sur les systèmes HP-UX, un pilote de passage SCSI est utilisé pour gérer le contrôleur et le périphérique de contrôle SCSI (aussi appelé robots ou sélectionneur) *des* périphériques de bibliothèque de bandes (comme 12000e). Le périphérique de contrôle est une bibliothèque responsable du chargement/déchargement du support vers/depuis les lecteurs et de l'importation/exportation du support vers/depuis ce périphérique.

Périphériques contrôlés en SCSI



Dispositifs de gestion



Le type de pilote de robot SCSI utilisé dépend du hardware. Les systèmes équipés de bus `GSC/HSC` ou `PCI` disposent d'un pilote de changeur automatique SCSI nommé `schgr`, et les systèmes équipés du bus `EISA` disposent du pilote de passage SCSI nommé `sctl` et déjà incorporé dans le noyau. Cependant, le pilote de passage SCSI utilisé sur les serveurs dotés d'un bus NIO est appelé `spt`. Il est installé sur le système sans être incorporé par défaut dans le noyau.

Si le pilote de robot SCSI n'est pas déjà lié à votre noyau actuel, vous devez l'ajouter vous-même et l'assigner aux robots connectés aux bibliothèques à bandes.

Les étapes ci-dessous expliquent comment ajouter *manuellement* le pilote de robot SCSI au noyau et comment en reconstruire un nouveau manuellement.

> **CONSEIL :**
> Sur une plateforme HP-UX, vous pouvez aussi construire le noyau avec l'utilitaire *Gestionnaire d'administration système (SAM)* de. Voir Installation de clients HP-UX , Page 71.

Utilisez la commande `/opt/omni/sbin/ioscan -f` pour vérifier si le pilote de robot SCSI est bien assigné à la bibliothèque que vous voulez configurer.

Statut du pilote de passage SCSI (sctl)

```
root@superhik$ ioscan -f
Class       I  H/W Path    Driver      S/W State H/W Type  Description
=============================================================
bc          0              root        CLAIMED   BUS_NEXUS
bc          1  8           ccio        CLAIMED   BUS_NEXUS I/O Adapter
unknown    -1  8/0                     CLAIMED   DEVICE    GSC-to-PCI Bus Bridge
ext_bus     0  8/12          c720      CLAIMED   INTERFACE GSC Fast/Wide SCSI Interfac
e
target      0  8/12.0        tgt       CLAIMED   DEVICE
disk        0  8/12.0.0      sdisk     CLAIMED   DEVICE    SEAGATE ST19171W
target      1  8/12.1        tgt       CLAIMED   DEVICE
tape        5  8/12.1.0      stape     CLAIMED   DEVICE    QUANTUM DLT7000
target      2  8/12.2        tgt       CLAIMED   DEVICE
ctl         0  8/12.2.0      sctl      CLAIMED   DEVICE    EXABYTE EXB-210
target      3  8/12.7        tgt       CLAIMED   DEVICE
ctl         0  8/12.7.0      sctl      CLAIMED   DEVICE    Initiator
ba          0  8/16          bus_adapter CLAIMED BUS_NEXUS Core I/O Adapter
ext_bus     2  8/16/0        CentIf    CLAIMED   INTERFACE Built-in Parallel Interface
audio       0  8/16/1        audio     CLAIMED   INTERFACE Built-in Audio
tty         0  8/16/4        asio0     CLAIMED   INTERFACE Built-in RS-232C
ext_bus     1  8/16/5        c720      CLAIMED   INTERFACE Built-in SCSI
target      4  8/16/5.2      tgt       CLAIMED   DEVICE
disk        2  8/16/5.2.0    sdisk     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-5401TA
target      7  8/16/5.3      tgt       NO_HW     DEVICE
tape        3  8/16/5.3.0    stape     NO_HW     DEVICE    SONY     SDX-300C
target      6  8/16/5.5      tgt       NO_HW     DEVICE
tape        0  8/16/5.5.0    stape     NO_HW     DEVICE    SONY     SDX-300C
target      5  8/16/5.7      tgt       CLAIMED   DEVICE
```

Statut du pilote de passage SCSI (sctl), Page précédente vous permet de voir que le pilote de passage SCSI `sctl` est assigné au périphérique de contrôle du lecteur de bandes Exabyte. Le chemin matériel concordant (chemin H/W) est `8/12.2.0`. (SCSI=2, LUN=0)

Il y a également un lecteur de bandes connecté au même bus SCSI, mais le pilote qui le contrôle est `stape`. Le chemin matériel concordant (chemin H/W) 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 toujours dans les résultats de la commande `ioscan -f`. Dans cet exemple, le contrôleur est géré par `sctl`.

Statut du pilote de passage SCSI (spt)

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
=============================================================
bc          0            root      CLAIMED   BUS_NEXUS
ext_bus     0  52        scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1      target    CLAIMED   DEVICE
disk        4  52.1.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2      target    CLAIMED   DEVICE
disk        0  52.2.0    disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4      target    CLAIMED   DEVICE
tape        0  52.4.0    tape2     CLAIMED   DEVICE    HP       C1533A
spt         1  52.4.1    spt       CLAIMED   DEVICE    HP       C1553A
target      6  52.5      target    CLAIMED   DEVICE
disk        5  52.5.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6      target    CLAIMED   DEVICE
disk        1  52.6.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56        lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0      mux4      CLAIMED   INTERFACE
lan         0  56.1      lan3      CLAIMED   INTERFACE
lantty      0  56.2      lantty0   CLAIMED   INTERFACE
processor   0  62        processor CLAIMED   PROCESSOR Processor
memory      0  63        memory    CLAIMED   MEMORY    Memory
# 
```

Statut du pilote de passage SCSI (spt), Page précédente vous donne un exemple de lecteur de bandes connecté contrôlé par le pilote de passage SCSI `spt`. Il s'agit là d'un périphérique de bibliothèque de bandes 12000e qui utilise l'adresse SCSI 4 et qui est connecté au bus SCSI avec le chemin H/W 52. Le chemin matériel concordant est 52.4.1. Les robots sont correctement assignés au pilote de passage SCSI `spt`.

Si le pilote `sctl`, `spt`, ou `schgr` n'est pas assigné aux robots, vous devez ajouter le chemin H/W des robots à la déclaration du pilote dans le fichier `system` et reconstruire le noyau. Suivez les instructions ci-dessous.

La procédure suivante explique comment ajouter *manuellement* un pilote de robot SCSI au noyau, l'assigner aux robots, puis reconstruire manuellement un nouveau noyau :

1. Connectez-vous en tant qu'utilisateur *root* et passez dans le répertoire de la version :

   ```
   cd /stand/build
   ```

2. Créez un nouveau fichier système depuis votre noyau existant :

   ```
   /usr/lbin/sysadm/system_prep -s system
   ```

3. Vérifiez que le pilote de robot SCSI est déjà intégré à votre noyau actuel. Depuis le répertoire `/stand`, exécutez la commande suivante :

   ```
   grep SCSIRoboticDriver system
   ```

   où le pilote *SCSIRoboticDriver* peut être `spt`, `sctl`, ou `schgr`. Le système va afficher la ligne correspondant si le pilote est déjà intégré au noyau actuel.

4. Utilisez un éditeur pour ajouter la déclaration du pilote :

   ```
   driver H/W Path spt
   ```

   au fichier `/stand/build/system`, où *H/W Path* est le chemin matériel complet du périphérique.

   Pour la bibliothèque de bandes 12000e de l'exemple précédent, vous devriez entrer :

   ```
   driver 52.4.1 spt
   ```

   Si plusieurs bibliothèques sont connectées au même système, vous devez ajouter une ligne de pilote avec le chemin matériel correspondant pour chaque robot de bibliothèque.

   Au moment de configurer le pilote `schgr`, ajoutez la ligne suivante à la déclaration de pilote :

   ```
   schgr
   ```

5. Entrez la commande `mk_kernel -s./system` pour construire un nouveau noyau.
6. Enregistrez le système d'origine sous un nom différent et déplacez le nouveau fichier système dans le nom d'origine pour qu'il remplace l'actuel :

   ```
   mv /stand/system /stand/system.prev
   mv /stand/build/system /stand/system
   ```

7. Enregistrez l'ancien noyau sous un nom différent et déplacez le nouveau noyau dans le nom d'origine pour qu'il remplace l'actuel :

   ```
   mv /stand/vmunix /stand/vmunix.prev
   mv /stand/vmunix_test /stand/vmunix
   ```

8. Redémarrez le système depuis le nouveau noyau avec la commande suivante :

   ```
   shutdown -r 0
   ```

9. Une fois le système redémarré, utilisez la commande `/usr/sbin/ioscan -f` pour vérifier les changements effectués.

Créer des fichiers de périphérique sur des systèmes HP-UX

Conditions préalables

Avant de créer un fichier de périphérique, assurez-vous qu'un périphérique de sauvegarde est déjà connecté au système. Utilisez la commande `/usr/sbin/ioscan -f` pour vérifier qu'un périphérique est bien connecté. Utilisez la commande `/usr/sbin/infs -e` pour créer automatiquement des fichiers de périphériques pour des périphériques de sauvegarde.

Si les fichiers de périphérique qui correspondent à un périphérique de sauvegarde précis n'ont pas été créés lors de l'initialisation (démarrage) du système ou après utilisation de la commande `infs -e`, vous devez les créer manuellement. C'est le cas avec les fichiers de périphérique nécessaires à la gestion du périphérique de contrôle de la bibliothèque (robot de bibliothèque).

Nous utiliserons en exemple la création d'un fichier de périphérique pour les robots du périphérique de sauvegarde 12000e connecté à un système HP-UX. Le fichier de périphérique du lecteur de bande a déjà été automatiquement créé après le redémarrage du système, alors que le fichier de périphérique du périphérique de contrôle doit être créé manuellement.

Statut du pilote de passage SCSI (spt), Page 375 permet de voir la sortie de la commande `ioscan -f` sur le système HP-UX sélectionné.

Liste des périphériques connectés

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
=============================================================
bc          0           root      CLAIMED   BUS_NEXUS
ext_bus     0  52        scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1      target    CLAIMED   DEVICE
disk        4  52.1.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2      target    CLAIMED   DEVICE
disk        0  52.2.0    disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4      target    CLAIMED   DEVICE
tape        0  52.4.0    tape2     CLAIMED   DEVICE    HP       C1533A
spt         1  52.4.1    spt       CLAIMED   DEVICE    HP       C1553A
target      6  52.5      target    CLAIMED   DEVICE
disk        5  52.5.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6      target    CLAIMED   DEVICE
disk        1  52.6.0    disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56        lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0      mux4      CLAIMED   INTERFACE
lan         0  56.1      lan3      CLAIMED   INTERFACE
lantty      0  56.2      lantty0   CLAIMED   INTERFACE
processor   0  62        processor CLAIMED   PROCESSOR Processor
memory      0  63        memory    CLAIMED   MEMORY    Memory
#
```

L'interface du bus SCSI est contrôlée par le pilote système `scsi1`. C'est une interface `SCSI NIO`. Pour accéder aux robots de bibliothèque sur le bus SCSI `SCSI NIO`, il faut utiliser le pilote de passage SCSI `spt` déjà installé et assigné au lecteur de bandes 12000e qui 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 requis et le pilote `sctl` est utilisé à la place.

Pour créer le fichier de périphérique, vous devez connaître le *Numéro majeur* du pilote de passage SCSI et le *Numéro mineur*, qui est indépendant du pilote de passage SCSI que vous utilisez.

Pour obtenir le *Numéro majeur* du `spt`, , utilisez la commande système suivante :

```
lsdev -d spt
```

Dans notre exemple (voir Liste des périphériques connectés, Page précédente), la commande a indiqué que le *Numéro majeur* était `75`.

Pour obtenir le *Numéro majeur* du `sctl`, utilisez la commande système suivante :

```
lsdev -d sctl
```

Dans notre cas, la commande a indiqué que le *Numéro majeur* était `203`.

Le *Numéro mineur*, quel que soit le pilote de passage SCSI utilisé, a toujours le format suivant :

```
0xIITL00
```

`II` -> Le *Numéro d'instance* de l'interface de bus SCSI (et PAS du périphérique) indiqué par le résultat de `ioscan -f` se trouve dans la deuxième colonne et porte l'étiquette `I`. Dans l'exemple, le numéro d'instance est `0`. Nous devons donc entrer deux chiffres hexadécimaux : 00.

`T` -> L'adresse SCSI des robots de bibliothèque. Dans l'exemple, l'adresse SCSI est `4`. Nous devons donc entrer `4`.

`L` -> Le numéro LUN des robots de bibliothèque. Dans l'exemple, le numéro LUN est `1`. Nous devons donc entrer `1`.

`00` -> Deux zéros hexadécimaux.

Créer un fichier de périphérique

La commande suivante est utilisée pour créer le fichier de périphérique :

```
mknod /dev/spt/devfile_name c Major # Minor #
```

Les fichiers de périphérique de `spt` sont généralement situés dans le répertoire `/dev/spt` ou `/dev/scsi`. Dans le cas présent, nous nommerons le fichier du périphérique de contrôle `/dev/spt/SS12000e`.

La commande complète pour créer le fichier de périphérique nommé `SS12000e` et situé dans le répertoire `/dev/spt` est donc :

```
mknod /dev/spt/SS12000e c 75 0x004100
```

Si nous créons un fichier de périphérique pour `sctl`, nommé SS12000e et situé dans le répertoire `/dev/scsi`, la commande complète est :

```
mknod /dev/scsi/SS12000e c 203 0x004100
```

Réglages des paramètres du contrôleur SCSI

Data Protector vous permet de changer la taille des blocs d'un périphérique, ce qui peut demander une configuration plus poussée sur certains contrôleurs SCSI.

Sur les systèmes Windows, paramétrez le contrôleur SCSI en éditant la valeur de registre pour les contrôleurs Adaptec SCSI, et pour certains contrôleurs équipés de puces Adaptec :

1. Configurez la valeur du registre suivante :`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aic78xx\Parameters\Device0\MaximumSGList`
2. Entrez une valeur `DWORD` égale au nombre de blocs 4 kB, plus un.

   `MaximumSGList = (OBBlockSize in kB / 4) + 1`

   Par exemple, pour permettre aux tailles de blocs d'aller jusqu'à 260 kB, `MaximumSGList` doit être au moins à `(260 / 4) + 1 = 66`.
3. Redémarrez le système.

> **REMARQUE :**
> Cette valeur de registre paramètre la limite haute de la taille des blocs. La taille actuelle des blocs d'un périphérique doit être configurée avec l'interface graphique de Data Protector prévue pour configurer les périphériques.

Recherche des adresses SCSI inutilisées sur les systèmes HP-UX

Un périphérique de sauvegarde connecté à un système HP-UX est accédé et contrôlé grâce à un fichier de périphérique. Il en faut un pour chaque périphérique physique. Avant de créer le fichier de périphérique, vous devez trouver quelles adresses SCSI (ports) sont actuellement inutilisées et disponibles.

Sur les systèmes HP-UX, la commande système `/usr/sbin/ioscan -f` permet d'afficher la liste des adresses SCSI en cours d'utilisation. Les adresses qui n'apparaissent pas dans le résultat de la commande `/usr/sbin/ioscan -f` sont donc actuellement inutilisées.

Dans Résultat de la commande ioscan -f utilisée sur un système HP-UX, bas, vous trouverez la sortie de la commande `/usr/sbin/ioscan -f` sur un système HP-UX 11.x.

Résultat de la commande ioscan -f utilisée sur un système HP-UX

```
# ioscan -f
Class       I  H/W Path  Driver    S/W State H/W Type  Description
===========================================================================
bc          0           root      CLAIMED   BUS_NEXUS
ext_bus     0  52       scsi1     CLAIMED   INTERFACE HP 28655A - SCSI Interface
target      4  52.1     target    CLAIMED   DEVICE
disk        4  52.1.0   disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      1  52.2     target    CLAIMED   DEVICE
disk        0  52.2.0   disc3     CLAIMED   DEVICE    TOSHIBA CD-ROM XM-4101TA
target      3  52.4     target    CLAIMED   DEVICE
tape        0  52.4.0   tape2     CLAIMED   DEVICE    HP       C1533A
spt         1  52.4.1   spt       CLAIMED   DEVICE    HP       C1553A
target      6  52.5     target    CLAIMED   DEVICE
disk        5  52.5.0   disc3     CLAIMED   DEVICE    SEAGATE ST15150N
target      2  52.6     target    CLAIMED   DEVICE
disk        1  52.6.0   disc3     CLAIMED   DEVICE    SEAGATE ST15150N
lanmux      0  56       lanmux0   CLAIMED   INTERFACE LAN/Console
tty         0  56.0     mux4      CLAIMED   INTERFACE
lan         0  56.1     lan3      CLAIMED   INTERFACE
lantty      0  56.2     lantty0   CLAIMED   INTERFACE
processor   0  62       processor CLAIMED   PROCESSOR Processor
memory      0  63       memory    CLAIMED   MEMORY    Memory
#
```

Seules les troisième et cinquième colonnes `(H/W Path)` et `(S/W State)` servent à déterminer les adresses SCSI disponibles. Un format `(H/W Path)` démembré devrait ressembler à ::

SCSI_bus_H/W_Path. SCSI_address. LUN_number

Dans ce cas en particulier, un seul bus SCSI utilise le chemin H/W 52. Sur ce bus, vous pouvez utiliser les adresses SCSI `0` et 3 parce qu'elles n'apparaissent pas dans la liste.

Vous pouvez voir dans Résultat de la commande ioscan -f utilisée sur un système HP-UX, Page précédente les adresses SCSI du bus SCSI sélectionné qui sont en cours d'utilisation :

- Adresse SCSI 1 par un disque SCSI
- Adresse SCSI 2 par un CD-ROM
- Adresse SCSI 4 LUN 0 par un lecteur de bandes
- Adresse SCSI 4 LUN 1 par les robots de la bibliothèque de bandes
- Adresse SCSI 5 par un disque SCSI
- Adresse SCSI 6 par un disque SCSI
- Adresse SCSI 7 par un contrôleur SCSI

> **REMARQUE :**
> L'adresse SCSI numéro 7 n'est *pas* listée bien qu'elle soit, par défaut, utilisée par le contrôleur SCSI.

Pour tous les périphériques, la valeur de `S/W State` est `CLAIMED` et celle de `H/W Type` est `H/W DEVICE`, ce qui indique qu'ils sont actuellement connectés. Si la valeur de `S/W State` avait été `UNCLAIMED` ou si celle de `H/W Type` avait été `NO-HW`, cela aurait voulu dire que le système ne pouvait accéder au périphérique.

L'adresse SCSI 4 est occupée par la bibliothèque de bandes qui a un lecteur de bandes avec LUN 0 et des robots avec LUN 1. Le lecteur est contrôlé par le pilote `tape2` et les robots sont contrôlés par le pilote de passage SCSI `spt` . La description vous permet de voir que le périphérique est une bibliothèque 12000e. C'est une bibliothèque SCSI facile à reconnaitre parce qu'elle utilise la même adresse SCSI mais des LUNs différents pour son lecteur de bandes et ses robots.

Le bus SCSI tout entier est contrôlé par le module d'interface `scsi1`.

Recherche des adresses SCSI inutilisées sur les systèmes Solaris

L'accès et le contrôle d'un périphérique de sauvegarde connecté à un système Solaris se fait grâce à un fichier de périphérique. Ce périphérique est automatiquement créé par le système d'exploitation Solaris dans le répertoire `/dev/rmt` quand le périphérique de sauvegarde est connecté et que le système client et le périphérique sont allumés.

Cependant, avant que le périphérique de sauvegarde ne soit connecté, les adresses SCSI disponibles doivent être identifiées et le périphérique de sauvegarde doit recevoir une adresse qui n'est pas déjà utilisée.

Pour voir les adresses SCSI disponibles sur un système Solaris

1. Éteignez le système en pressant **Stop** et **A**.
2. Exécutez la commande `probe-scsi-all` à l'invite `ok` :

   ```
   probe-scsi-all
   ```

   Le système peut vous demander de lancer la commande `probe-scsi-all` avant d'exécuter la commande `reset-all`.
3. Pour revenir à la normale, entrez `go` à l'invite `ok` :

   ```
   go
   ```

Une fois les adresses disponibles obtenues et une fois que vous avez choisi celle que vous comptez utiliser pour le périphérique de sauvegarde, vous devez mettre à jour les fichiers de configuration correspondants avant de connecter et de démarrer le périphérique. Reportez-vous à la prochaine section pour connaitre les instructions pour mettre à jour les fichiers de configuration.

Mise à jour de la configuration du périphérique et du lecteur sur les systèmes Solaris

Mettre à jour des fichiers de configuration

Les fichiers de configuration suivants sont utilisés pour la configuration d'un périphérique et d'un pilote. Ils doivent être vérifiés et édités si nécessaire avant utilisation des périphériques attachés :

- `st.conf`
- `sst.conf`

st.conf: tous périphériques

Ce fichier doit se trouver sur chaque client Data Protector Solaris équipé d'un lecteur de bandes. Il doit contenir les informations relatives au périphérique et une ou plusieurs adresses SCSI pour chaque périphérique de sauvegarde connecté au client. Un périphérique à lecteur unique requiert une seule entrée SCSI alors qu'un périphérique de bibliothèque multilecteurs en nécessite plusieurs.

1. Utilisez la méthode décrite dans la section précédente pour vérifier les adresses SCSI inutilisées sur le client et en choisir une pour le périphérique que vous souhaitez attacher.
2. Configurer la ou les adresses SCSI choisies sur le périphérique de sauvegarde.
3. Éteignez le système du client.
4. Attachez le périphérique de sauvegarde.
5. Allumez d'abord le périphérique puis le système du client.
6. Éteignez le système en appuyant sur `Stop` et `A`.
7. Saisissez la commande `probe-scsi-all` à l'invite `ok` :

   ```
   probe-scsi-all
   ```

   Vous obtenez des informations sur les périphériques SCSI connectés, y compris la chaîne ID du nouveau périphérique de sauvegarde.
8. Retournez à la normale en lançant :

go

9. Modifiez le fichier `/kernel/drv/st.conf`. Ce fichier est utilisé par le pilote `st` (bandes SCSI) de Solaris. Il contient la liste des périphériques officiellement pris en charge par Solaris et des entrées de configurations pour des périphériques tiers. Si vous utilisez un périphérique pris en charge, il devrait être possible de le connecter et de l'utiliser sans configuration supplémentaire. Dans le cas contraire, ajoutez les types d'entrées suivantes à `st.conf` :
   - Une entrée dans la liste de configuration sur bande (plus une définition de variable de données sur bande). Des exemples d'entrées sont fournis et commentés dans le fichier. Vous pouvez les utiliser ou les modifier selon vos besoins.

     L'entrée doit venir avant la première entrée `name=` du fichier et le format est le suivant:

     tape-config-list= "*Tape unit*", "*Tape reference name*", "*Tape data*";

     où :

Tape unit	La chaîne ID de l'éditeur et du produit pour le lecteur de bandes. Elle doit être spécifiée correctement comme indiqué dans la documentation du fabriquant.
Tape reference name	Le nom que vous choisissez et que le système utilisera pour identifier le lecteur de bandes. Le nom que vous fournissez ne change pas l'ID du produit, mais le nom de référence sera affiché dans la liste des périphériques reconnus par le système quand celui-ci démarrera.
Tape data	Une variable qui référence une série d'objets de configuration supplémentaires du lecteur de bandes. La définition de la variable doit aussi être fournie et spécifiée correctement, comme indiqué dans la documentation du fabriquant.

     Par exemple :

     `tape-config-list= “Quantum DLT4000”, “Quantum DLT4000”, “DLT-data”;`

     `DLT-data = 1,0x38,0,0xD639,4,0x80,0x81,0x82,0x83,2;`

     Le deuxième paramètre `0x38` appelle le type de bande DLTtape «autre lecteur SCSI». La valeur spécifiée ici doit être définie dans `/usr/include/sys/mtio.h`.

     > **REMARQUE :**
     > Assurez-vous que la dernière entrée de tape-config-list est terminée par un point virgule (;).

   - Pour les périphériques multilecteurs, ciblez les entrées suivantes :

     `name="st" class="scsi"`

     `target=X lun=Y;`

     où :

X	est le port SCSI assigné au lecteur de données (ou mécanisme de robot).
Y	est la valeur logique de l'unité.

     Par exemple :

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

```
name="st" class="scsi"
 target=2 lun=0
```

Normalement les entrées cible ne sont requises dans `st.conf` que pour les lecteurs. Le mécanisme des robots est sur une différente cible. Leurs entrées sont généralement fournies dans le fichier `sst.conf` (voir ci-dessous). Il existe cependant des périphériques, par exemple le 24x6, qui traitent le mécanisme des robots comme un autre lecteur. Dans ce cas, deux entrées avec la même cible sont requises (une pour le lecteur et une pour les robots), mais avec des LUNs différentes

Par exemple :

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

sst.conf: périphériques de bibliothèque

Ce fichier est requis sur chaque client Data Protector Solaris avec un périphérique de bibliothèque multilecteur connecté. En général, il faut une entrée pour l'adresse SCSI du mécanisme des robots de chaque périphérique de bibliothèque connecté au client (il existe des exceptions, comme le 24x6 mentionné plus tôt).

1. Copiez dans le répertoire demandé le pilote (module) `sst` et le fichier de configuration `sst.conf` :
   - Pour les systèmes d'exploitation en 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 en 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. Éditez le fichier `sst.conf` et ajoutez l'entrée suivante :

   ```
   name="sst" class="scsi" target=X lun=Y;
   ```

   où :

X	et l'adresse SCSI du mécanisme des robots.
Y	est l'unité logique.

   Par exemple :

   ```
   name="sst" class="scsi" target=6 lun=0;
   ```

3. Ajoutez le pilote au noyau Solaris :

   ```
   add_drv sst
   ```

Créer et contrôler des fichiers de périphérique

Une fois les fichiers de configuration paramétrés et les pilotes installés, vous pouvez créer les fichiers de périphériques comme indiqué :

1. Supprimez tous les fichiers de périphérique existants du répertoire `/dev/rmt`.

   ```
   cd /dev/rmt rm *
   ```

2. Entrez ce qui suit pour éteindre le système :

   ```
   shutdown -i0 -g0
   ```

3. Redémarrez le système.

   ```
   boot -rv
   ```

   Le paramètre `r` de la commande `boot` permet la compilation du noyau et la création de fichiers de périphérique spéciaux pour communiquer avec le lecteur de bandes. Le paramètre `v` active le démarrage documenté du système. En mode documenté, le système devrait afficher, pendant la phase du démarrage dédiée à la configuration du répertoire `/devices`, la chaîne *nom de référence de la bande* (celle que vous avez choisie) pour indiquer que le périphérique est bien activé.

4. Entrez les commandes suivantes pour vérifier l'installation :

   ```
   mt -t /dev/rmt/0 status
   ```

   Le résultat de cette commande dépend du lecteur configuré. Il devrait ressembler à :

   ```
   Quantum DLT7000 tape drive: sense key(0x6)= Unit Attention residual= 0 retries=
   0 file no= 0 block no= 0
   ```

5. Une fois le système redémarré, vous pouvez utiliser la commande `ls -all.` pour vérifier que les fichiers de périphérique ont bien été créés.Dans le cas d'un périphérique de bibliothèque, le résultat de la commande devrait donner :

`/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

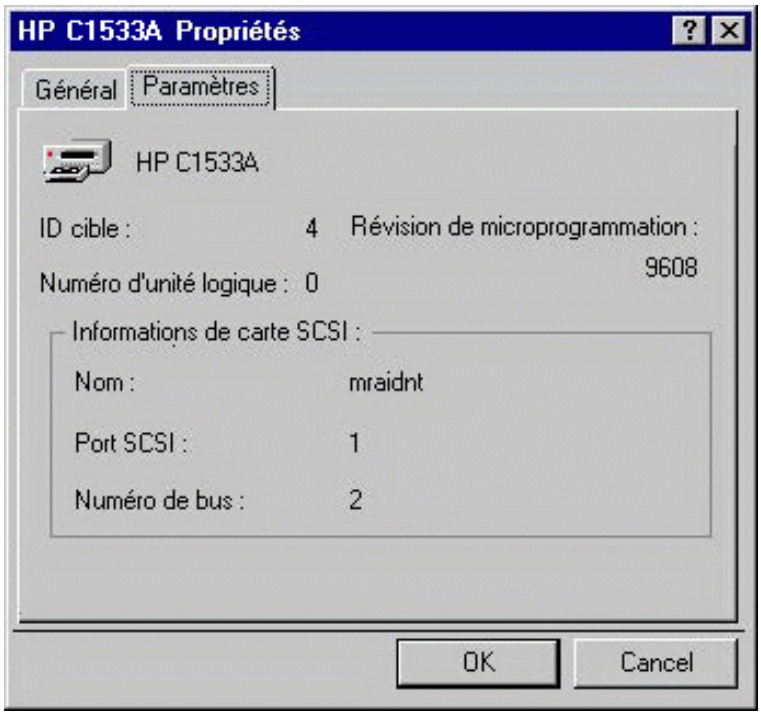
Recherche des ID SCSI inutilisés sur les systèmes Windows

Pour trouver des ID cibles SCSI inutilisées (adresses SCSI) sur un système Windows

1. Dans le Panneau de configuration Windows, cliquez sur **Adaptateurs SCSI**.
2. Contrôlez les propriétés de chaque périphérique connecté à un adaptateur SCSI. Cliquez deux fois sur le nom d'un périphérique, puis sélectionnez **Paramètres** pour ouvrir les propriétés. Voir Paramètres d'un périphérique, bas.

   Notez les `SCSI Target IDs` et les `LUNs(Logical Unit Numbers)` attribuées au périphérique. De cette manière vous pouvez trouver quelles `SCSI Target ID` et `LUNs` sont en cours d'utilisation.

Paramètres d'un périphérique



Configuration des ID SCSI sur une bibliothèque 330fx

Une fois les ID SCSI inutilisées choisies pour les robots et les lecteurs, vous pouvez les contrôler et les configurer grâce au Panneau de configuration du périphérique de bibliothèque.

Exemple

Si vous possédez un modèle de bibliothèque 330fx, vous pouvez trouver les ID SCSI configurées de cette manière :

1. Depuis READY, appuyez sur **NEXT** pour faire apparaître `ADMIN*`.
2. Appuyez sur **ENTER** pour faire apparaître une demande de mot de passe. Entrez le mot de passe.
3. `TEST*` apparaitra, appuyez sur **NEXT** jusqu'à ce que `SCSI IDs *` apparaisse.
4. Appuyez sur **Entrée**. `VIEW IDs*` s'affiche.
5. Appuyez sur **Entrée**. `JKBX ID 6 LUN 0` s'affiche.
6. Appuyez sur **NEXT**. `DRV 1 ID 5 LUN 0` s'affiche.
7. Appuyez sur **NEXT**. `DRV 2 ID 4 LUN 0` apparait, etc.

Appuyez plusieurs fois sur CANCEL pour revenir à `READY`.

Connexion des périphériques de sauvegarde

La procédure suivante décrit la marche à suivre pour connecter un périphérique de sauvegarde à un système HP-UX, Solaris, Linux ou Windows.

1. Sélectionnez le client auquel vous voulez connecter le périphérique de sauvegarde.
2. Installez l'Agent de support sur le système sélectionné. Voir Installation à distance, Page 95.
3. Déterminez l'adresse SCSI inutilisée que le périphérique pourra utiliser. Pour les systèmes HP-UX, voir Recherche des adresses SCSI inutilisées sur les systèmes HP-UX, Page 379. Pour les systèmes Solaris, voir Recherche des adresses SCSI inutilisées sur les systèmes Solaris, Page 380. Pour un système Windows, voir Recherche des ID SCSI inutilisés sur les systèmes Windows, Page 384.
   - Si vous connectez le périphérique sur un système HP-UX, vérifiez que les pilotes requis sont *installés* et *intégrés* au noyau actuel. Voir Vérifier la configuration du noyau sur HP-UX, Page 73.

     Si vous avez besoin de configurer un pilote de passage SCSI, reportez-vous à Configuration de robotiques SCSI sur systèmes HP-UX, Page 373.

   - Si vous connectez le périphérique à un système Solaris, vérifiez que les pilotes requis sont installés et que les fichiers de configurations sont à jour pour le périphérique à installer. Voir Mise à jour de la configuration du périphérique et du lecteur sur les systèmes Solaris, Page 381. Cela demande aussi de mettre à jour le fichier `sst.conf` si vous avez besoin de configurer un pilote de passage SCSI.

   - Si vous connectez le périphérique à un client Windows, le pilote de bandes d'origine peut être chargé ou désactivé, suivant la version du système Windows. Voir Utilisation de lecteurs bande et robotique sur systèmes Windows, Page 369.

     Si vous chargez le pilote de bandes d'origine pour un périphérique déjà configuré dans Data Protector et que vous n'avez pas utilisé le pilote de bandes d'origine, assurez-vous de bien renommer tous les noms de fichier de périphérique pour tous les périphériques logiques Data Protector configurés qui référencent ce périphérique en particulier (par exemple, changez `scsi1:0:4:0` en `tape3:0:4:0`).

     Pour plus d'informations sur les noms de fichiers de périphériques appropriés, consultez Créer des fichiers de périphérique (adresses SCSI) sur des systèmes Windows, Page 372.

4. Configurez les adresses (ID) SCSI sur le périphérique. En général, vous pouvez le faire avec les boutons du périphérique - suivant son type -. Pour plus de détails, consultez la documentation fournie avec le périphérique.

   Pour consulter un exemple, voir Configuration des ID SCSI sur une bibliothèque 330fx, Page précédente.

   Pour plus d'informations sur les périphériques pris en charge, reportez-vous à https://softwaresupport.softwaregrp.com/.

   > **REMARQUE :**
   > Sur un système Windows avec un adaptateur SCSI Adaptec et un périphérique SCSI connectés, l'option `Host Adapter BIOS` doit être activée pour que le système n'ait pas de

> problème lors de l'utilisation de commandes SCSI.
>
> Pour activer l'option BIOS adaptateur hôte, appuyez sur **Ctrl+A** pendant le démarrage du système pour accéder au menu Adaptateur SCSI, sélectionnez **Configurer/Voir les paramètres de l'adaptateur hôte > Options de configuration avancées** et activez l'option.

5. Allumez en premier le périphérique, puis l'ordinateur, puis attendez que le démarrage se termine. Vérifiez que le système reconnaisse bien votre nouveau périphérique de sauvegarde.

   Systèmes Windows : vous pouvez vérifier que le système reconnaisse bien votre nouveau périphérique de sauvegarde avec l'utilitaire `devbra`. Dans le répertoire des commandes Data Protector par défaut, exécutez la commande `devbra -dev`.

   Vous trouverez dans les résultats de la commande `devbra` les lignes suivantes pour chaque périphérique connecté et reconnu :

   spécification de périphérique de sauvegarde

   chemin_matériel

   type_de_support

   .....

   Par exemple :

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

   signifie qu'un lecteur de bandes DDS (avec un pilote de bandes d'origine chargé) possède le numéro d'instance de lecteur 3, est connecté au bus SCSI 0, et possède l'ID cible SCSI 4 et le LUN 0.

   Ou le résultat suivant :

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

   signifie qu'un lecteur de bandes DDS (avec un pilote de bandes d'origine chargé) est connecté au port SCSI 1, bus SCSI 0, et que le lecteur de bandes possède l'ID cible SCSI 4 et le LUN 0.

   Systèmes HP-UX : Exécutez la commande `/usr/sbin/ioscan -fn` pour afficher la liste des périphériques connectés - avec leur chemin matériel et leur fichier de périphérique - qui vous permettra de trouver votre périphérique nouvellement connecté grâce aux adresses SCSI correctes.

   Si le fichier de périphérique n'a pas été créé automatiquement pendant le démarrage du système, vous devrez le créer manuellement. Voir Créer des fichiers de périphérique sur des systèmes HP-UX, Page 377.

Systèmes Solaris : exécutez la commande `ls -all` dans le répertoire `/dev/rmt` pour afficher la liste des périphériques connectés - avec leur chemin matériel et leur fichier de périphérique - qui vous permettra de trouver votre périphérique nouvellement connecté grâce aux adresses SCSI correctes.

Systèmes Linux : Exécutez la commande `ls -all` dans le répertoire `/dev/rmt` pour afficher la liste des périphériques connectés - avec leur chemin matériel et leur fichier de périphérique - qui vous permettra de trouver votre périphérique nouvellement connecté grâce aux adresses SCSI correctes.

Système AIX : Exécutez la commande `lsdev -C` pour afficher la liste des périphériques connectés avec les fichiers de périphérique correspondants.

Compression matérielle

La plupart des périphériques de sauvegarde récents proposent une compression matérielle intégrée qui peut être activée pendant la création d'un fichier de périphérique ou d'une adresse SCSI au cours de la procédure de configuration du périphérique. Pour plus d'informations, reportez-vous à la section *Aide de Data Protector*.

La compression matérielle est effectuée par un périphérique qui reçoit les données originales de l'Agent de support et les écrit sur la bande en mode compressé. Ce procédé permet d'augmenter la vitesse à laquelle un lecteur de bande reçoit les données car le volume de données écrit sur la bande est moins important.

Quand la compression logicielle est utilisée et que la compression matérielle est désactivée, les données sont compressées par l'Agent de disque et envoyées à un Agent de support. L'algorithme de compression peut prendre une quantité conséquente de ressources au système de l'Agent de disque si la compression logicielle est utilisée, mais le procédé réduit la charge sur le 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 de bandes est chargé). Si le périphérique prend en charge la compression matérielle, celle-ci sera utilisée ; sinon, l'option C sera ignorée.

Pour désactiver la compression matérielle sous Windows, ajoutez N à la fin des adresses SCSI de périphérique/lecteur. Par exemple : scsi:0:3:0:N.

Pour activer/désactiver la compression matérielle sous UNIX, sélectionnez un fichier de périphérique approprié. Pour plus de détails à ce sujet, consultez la documentation de votre système d'exploitation et celle de votre périphérique.

Étapes suivantes

Les périphériques de sauvegarde devraient maintenant être connectés et vous devriez pouvoir les configurer et configurer les pools de support. Pour plus d'informations au sujet de ces tâches de configuration, reportez-vous à l'index de *Aide de Data Protector* : "configuration, périphériques de sauvegarde".

Un Agent de support doit être installé sur votre système. Voir Installation à distance, Page 95.

Les sections suivantes décrivent comment connecter un lecteur de bandes HPE Standalone 24, une bibliothèque 12000e et une DLT Library 28/48-Slot sur un système HP-UX et un système Windows.

Connecter un périphérique indépendant HPE 24

Le périphérique de sauvegarde 24 DDS est un lecteur de bandes indépendant basé sur la technologie DDS3.

Connecter à un système HP-UX

Pour connecter un périphérique indépendant HPE 24 à un système HP-UX

1. Vérifiez que les pilotes requis (`stape` ou `tape2`) sont *installés* et *intégrés* au noyau actuel. Voir Vérifier la configuration du noyau sur HP-UX, Page 73.
2. Trouvez une adresse SCSI disponible utilisable par le lecteur de bandes. Voir Recherche des adresses SCSI inutilisées sur les systèmes HP-UX, Page 379.
3. Configurez les adresses (ID) SCSI sur le périphérique. Utilisez les boutons à l'arrière du périphérique.

   Pour plus de détails, consultez la documentation fournie avec le périphérique.
4. Allumez en premier le périphérique, puis l'ordinateur, puis attendez que le démarrage se termine.
5. Vérifiez que le système reconnaisse le lecteur de bandes nouvellement connecté. Utilisez l'utilitaire `ioscan` :

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

   pour afficher la liste des périphériques connectés - avec les chemins matériels et les fichiers de périphérique correspondants - où vous devriez trouver le lecteur de bandes nouvellement connecté qui a l'adresse SCSI correcte. Le fichier de périphérique du lecteur a bien été créé pendant le démarrage.

Étapes suivantes

Après avoir correctement connecté le périphérique, consultez l'index *Aide de Data Protector* : "configuration, périphériques de sauvegarde" afin d'obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour votre appareil nouvellement connecté.

Connecter à un système Windows

Pour connecter un périphérique indépendant HPE 24 à un système Windows

1. Trouvez une adresse SCSI (ID cible) disponible utilisable par le lecteur de bandes. Voir Recherche des ID SCSI inutilisés sur les systèmes Windows, Page 384.
2. Configurez les adresses (ID) SCSI sur le périphérique. Utilisez les boutons à l'arrière du périphérique. Pour plus de détails, consultez la documentation fournie avec le périphérique.
3. Allumez en premier le périphérique, puis l'ordinateur, puis attendez que le démarrage se termine.
4. Vérifiez que le système reconnaisse le lecteur de bandes nouvellement connecté. Dans le répertoire des commandes Data Protector par défaut, exécutez la commande `devbra -dev`.

   Dans les résultats de la commande `devbra`, vous devriez trouver le lecteur de bandes nouvellement connecté du périphérique indépendant HPE 24.

Et après ?

Après avoir correctement connecté le périphérique, consultez l'index *Aide de Data Protector* : "configuration, périphériques de sauvegarde" afin d'obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour votre appareil nouvellement connecté.

Connecter un Chargeur automatique DAT

Les bibliothèques 12000e et DAT24x6 possèdent un référentiel pour six cartouches, un lecteur, et un bras mécanique utilisé pour déplacer les cartouches vers et depuis le lecteur. Les deux bibliothèques possèdent également un détecteur de bandes sales intégré.

Connecter à un système HP-UX

Pour connecter le périphérique de bibliothèque 12000e à un système HP-UX

1. À l'arrière du chargeur automatique, mettez le bouton mode sur `6`.
2. Vérifiez que les pilotes requis (`stape` ou `tape2`) sont *installés* et *intégrés* au noyau actuel. Voir Vérifier la configuration du noyau sur HP-UX, Page 73.
3. Vérifiez que les pilotes de passage SCSI requis (`sctl` ou `spt` sont *installés* et *intégrés* au noyau actuel. Voir Configuration de robotiques SCSI sur systèmes HP-UX, Page 373.
4. Trouvez une adresse SCSI disponible utilisable par le lecteur de bandes et les robots. Voir Recherche des adresses SCSI inutilisées sur les systèmes HP-UX, Page 379.

   > **REMARQUE :**
   > La bibliothèque 12000e utilise la même adresse SCSI, mais des numéros LUN différents, pour le lecteur de bandes et les robots.

5. Configurez les adresses (ID) SCSI sur le périphérique. Pour plus de détails, consultez la documentation fournie avec le périphérique.
6. Allumez en premier le périphérique, puis l'ordinateur, puis attendez que le démarrage se termine.
7. Vérifiez que le système reconnaisse le lecteur de bandes nouvellement connecté. Utilisez l'utilitaire `ioscan`

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

   pour afficher la liste des périphériques connectés - avec les chemins matériels et les fichiers de périphérique correspondants - où vous devriez trouver le lecteur de bandes nouvellement connecté avec l'adresse SCSI correcte.
8. Le fichier de périphérique du lecteur de bandes a été créé pendant le démarrage, alors que le fichier de périphérique des robots doit être créé manuellement. Voir Créer des fichiers de périphérique sur des systèmes HP-UX, Page 377.
9. Vérifiez que le système reconnaisse correctement le fichier de périphérique nouvellement créé pour les robots de bibliothèque. Exécutez l'utilitaire `ioscan` :

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

   Vous devriez voir le fichier de périphérique nouvellement créé dans les résultats de la commande.

Étapes suivantes

Après avoir correctement connecté le périphérique de la bibliothèque, consultez l'index *Aide de Data Protector* : "configuration, périphériques de sauvegarde" afin d'obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour votre appareil nouvellement connecté.

Connecter à un système Windows

Pour connecter le périphérique de bibliothèque 12000e à un système Windows

1. À l'arrière du chargeur automatique, mettez le bouton mode sur `6`.
2. Trouvez une adresse SCSI disponible utilisable par le lecteur de bandes et les robots. Voir Recherche des ID SCSI inutilisés sur les systèmes Windows, Page 384.
3. Configurez les adresses (ID) SCSI sur le périphérique. Pour plus de détails, consultez la documentation fournie avec le périphérique.

   > **REMARQUE :**
   > La bibliothèque 12000e utilise la même adresse SCSI, mais des numéros LUN différents, pour le lecteur de bandes et les robots.

4. Allumez en premier le périphérique, puis l'ordinateur, puis attendez que le démarrage se termine.
5. Vérifiez que le système reconnaisse le lecteur de bandes et les robots nouvellement connectés. Dans le répertoire des commandes Data Protector par défaut, exécutez la commande `devbra -dev`.

   Dans les résultats de la commande `devbra`, vous devriez trouver le lecteur de bandes et les robots nouvellement connectés du périphérique de bibliothèque 12000e.

Étapes suivantes

Après avoir correctement connecté le périphérique de la bibliothèque, consultez l'index *Aide de Data Protector* : "configuration, périphériques de sauvegarde" afin d'obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour votre appareil nouvellement connecté.

Connecter une DLT Library 28/48-Slot

La DLT Library 28/48-Slot est une bibliothèque multilecteur pour entreprises possédant 80 à 600 GB de données 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.

Connecter à un système HP-UX

Pour connecter le périphérique de bibliothèque DLT Library 28/48-Slot à un système HP-UX

1. Vérifiez que les pilotes requis (`stape` ou `tape2`) sont *installés* et *intégrés* au noyau actuel. Voir Vérifier la configuration du noyau sur HP-UX, Page 73.
2. Vérifiez que les pilotes de passage SCSI requis (`sctl` ou `spt`) sont *installés* et *intégrés* au noyau actuel. Voir Configuration de robotiques SCSI sur systèmes HP-UX, Page 373.
3. Trouvez une adresse SCSI disponible utilisable par le lecteur de bandes et les robots. Voir Recherche des adresses SCSI inutilisées sur les systèmes HP-UX, Page 379.

   > **REMARQUE :**
   > La DLT Library 28/48-Slot possède quatre lecteurs de bandes et des robots. Il vous faut donc cinq adresses SCSI inutilisées au cas où vous souhaiteriez profiter de tous les lecteurs de bandes. Les lecteurs de bandes et les robots doivent utiliser des adresses SCSI différentes.

4. Configurez les adresses (ID) SCSI sur le périphérique. Pour plus de détails, consultez la documentation fournie avec le périphérique.
5. Tout d'abord, allumez le périphérique, puis l'ordinateur, et attendez que le démarrage se termine.
6. Vérifiez que le système reconnaisse les lecteurs de bandes nouvellement connectés. Utilisez l'utilitaire `ioscan`

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

   pour afficher une liste des périphériques connectés - avec les chemins matériels et les fichiers de périphérique correspondants - où vous devriez trouver vos lecteurs de bandes nouvellement connectés avec les adresses SCSI correctes.
7. Les fichiers de périphérique des lecteur ont été créés pendant le démarrage, alors que le fichier de périphérique des robots doit être créé manuellement. Voir Créer des fichiers de périphérique sur des systèmes HP-UX, Page 377.
8. Vérifiez que le système reconnaisse correctement le fichier de périphérique nouvellement créé pour les robots de bibliothèque. Utilisez l'utilitaire `ioscan` :

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

   Vous devriez voir le fichier de périphérique nouvellement créé dans les résultats de la commande.

Étapes suivantes

Après avoir correctement connecté le périphérique de bibliothèque DLT Library 28/48-Slot, consultez l'index *Aide de Data Protector* : "configuration, périphériques de sauvegarde" afin d'obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour votre appareil nouvellement connecté.

Connecter à un système Solaris

Pour cet exemple, nous considérerons que deux lecteurs sont alloués à Data Protector.

Pour connecter le périphérique de bibliothèque C5173-7000 à un système Solaris

1. Copiez dans le répertoire demandé le pilote (module) `sst` et le fichier de configuration `sst.conf` :
   - Pour les systèmes d'exploitation en 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 en 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. Éteignez le système en pressant **Stop** et `A.`
5. Exécutez la commande `probe-scsi-all` à l'invite "`ok`" pour vérifier quelles adresses SCSI sont 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 notre cas, nous utiliserons le port 6 pour le périphérique de contrôle SCSI, le port 2 pour le premier lecteur, et le port 1 pour le second lecteur (le LUN est 0).
6. Retournez à la normal en lançant :

   ```
   ok go
   ```

7. Copiez le fichier de configuration `st.conf` dans le bon répertoire :

   ```
   $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. Éditez le fichier `/kernel/drv/st.conf` et ajoutez l'entrée suivante :

   ```
   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, respectivement, le lecteur 1, le lecteur 2, et le lecteur de robots..
9. Éditez le fichier `sst.conf` (que vous avez copiez pendant l'Copiez dans le répertoire demandé le

pilote (module) sst et le fichier de configuration sst.conf :, haut) pour y ajouter la ligne suivante :

```
name="sst" class="scsi" target=6 lun=0;
```

> **REMARQUE :**
> Cette entrée doit correspondre à celle du lecteur de robots du fichier `st.conf`. Reportez-vous à la rubrique Éditez le fichier /kernel/drv/st.conf et ajoutez l'entrée suivante :, Page précédente plus haut.

10. Éteignez le système du client et connectez le périphérique de bibliothèque.
11. Allumez le périphérique de bibliothèque en premier, puis le système du client.

    Le système va démarrer et automatiquement créer les fichiers de périphérique pour le lecteur des robots et les lecteurs de bandes. Vous pouvez les afficher avec la commande `ls -all.` .Dans notre cas :

`/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

Et après ?

Après avoir correctement connecté le périphérique de bibliothèque DLT Library 28/48-Slot, consultez l'index *Aide de Data Protector* : "configuration, périphériques de sauvegarde" afin d'obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour votre appareil nouvellement connecté.

Connecter à un système Windows

Pour connecter le périphérique de bibliothèque DLT Library 28/48-Slot à un système Windows

1. Trouvez une adresse SCSI libre utilisable par le lecteur de bandes et les robots. Voir Recherche des ID SCSI inutilisés sur les systèmes Windows, Page 384.
2. Configurez les adresses (ID) SCSI sur le périphérique. Pour plus de détails, consultez la documentation fournie avec le périphérique.

   > **REMARQUE :**
   > La DLT Library 28/48-Slot possède quatre lecteurs de bandes et des robots. Il vous faut donc cinq adresses SCSI inutilisées au cas où vous souhaiteriez profiter de tous les lecteurs de bandes. Les lecteurs de bandes et les robots doivent utiliser des ID cibles SCSI différentes.

3. Allumez en premier le périphérique, puis l'ordinateur, puis attendez que le démarrage se termine.
4. Vérifiez que le système reconnaisse les lecteurs de bandes et les robots nouvellement connectés. Dans le répertoire des commandes Data Protector par défaut, exécutez la commande `devbra -dev`.

   Dans les résultats de la commande `devbra`, vous devriez trouver les lecteurs de bandes et les robots nouvellement connectés du périphérique de bibliothèque DLT Library 28/48-Slot.

Étapes suivantes

Après avoir correctement connecté le périphérique de bibliothèque DLT Library 28/48-Slot, consultez l'index *Aide de Data Protector* : "configuration, périphériques de sauvegarde" afin d'obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour votre appareil de bibliothèque nouvellement connecté.

Connecter un lecteur de bandes Seagate Viper 200 LTO Ultrium

Le lecteur de bandes Seagate Viper 200 LTO Ultrium est un périphérique indépendant pour entreprises possédant de 100 à 200 GB de données à sauvegarder.

Connecter à un système Solaris

Pour configurer le lecteur de bandes Seagate Viper 200 LTO Ultrium sur un système Solaris

1. Trouvez une adresse SCSI disponible utilisable par le lecteur de bandes. Exécutez la commande `modinfo` ou `dmesg` pour trouver les contrôleurs SCSI utilisés et les périphériques cibles SCSI installés :

   ```
   dmesg | egrep “target” | sort | uniq
   ```

   Le résultat suivant devrait s'afficher :

   ```
   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 un contrôleur SCSI `glm` ou `isp` quand vous connectez le périphérique Viper 200 LTO à un système Solaris. Il est également recommandé d'utiliser soit un contrôleur Ultra2 SCSI, soit un contrôleur Ultra3 SCSI.

2. Éditez le fichier `/kernel/drv/st.conf` et ajoutez l'entrée suivante :

   ```
   tape-config-list=
    “SEAGATE ULTRIUM06242-XXX” , “SEAGATE LTO” , \
    “SEAGATE_LTO”;
    SEAGATE_LTO = 1, 0x7a, 0, 0x1d679, 4, 0x00, 0x00, 0x00, \
    0x00, 1;
   ```

3. Éteignez le système du client et connectez le périphérique.
4. Allumez le périphérique en premier, puis le système du client.

   Le système va démarrer et automatiquement créer les fichiers de périphérique pour le lecteur de bandes. Vous pouvez les afficher avec la commande `ls -all`.

Et après ?

Après avoir correctement connecté le périphérique Seagate Viper 200 LTO Ultrium Tape Drive, consultez l'index *Aide de Data Protector* : "configuration, périphériques de sauvegarde" afin d'obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour votre appareil nouvellement connecté.

Connecter à un système Windows

Pour configurer le lecteur de bandes Seagate Viper 200 LTO Ultrium sur un système Windows

1. Trouvez une adresse SCSI (ID cible) disponible utilisable par le lecteur de bandes. Voir Recherche des ID SCSI inutilisés sur les systèmes Windows, Page 384.
2. Configurez les adresses (ID) SCSI sur le périphérique. Pour plus de détails, consultez la documentation fournie avec le périphérique.
1. Allumez en premier le périphérique, puis l'ordinateur, puis attendez que le démarrage se termine.
2. Vérifiez que le système reconnaisse les lecteurs de bandes et les robots nouvellement connectés. Dans le répertoire des commandes Data Protector par défaut, exécutez la commande `devbra -dev`.

   Dans les résultats de la commande `devbra`, vous devriez trouver le lecteur de bandes nouvellement connecté du lecteur de bandes Seagate Viper 200 LTO Ultrium.

Étapes suivantes

Après avoir correctement connecté le périphérique Seagate Viper 200 LTO Ultrium Tape Drive, consultez l'index *Aide de Data Protector* : "configuration, périphériques de sauvegarde" afin d'obtenir des instructions sur la configuration d'un périphérique de sauvegarde Data Protector pour votre appareil nouvellement connecté.

> **REMARQUE :**
> Quand vous configurez le lecteur de bandes Seagate Viper 200 LTO Ultrium avec Data Protector, assurez-vous que le mode de compression soit configuré. Vous pouvez le faire en ajoutant le paramètre `C` après l'adresse SCSI du lecteur. Par exemple :
>
> ```
> scsi2:0:0:0C
> ```

Annexe D: Plus d'informations

> **REMARQUE :**
> La documentation disponible sur le site Web du assistance clientèle à l'adresse contient les dernières mises à jour et correctionshttps://softwaresupport.softwaregrp.com/.

Vous pouvez accéder au kit de documentation Data Protector à partir des emplacements suivants :

- Répertoire d'installation de Data Protector.

  Systèmes Windows :*répertoire_Data_Protector*\docs

  Systèmes UNIX :/opt/omni/doc/C
- Menu **Aide** du GUI Data Protector .
- Site Web d'assistance à l'adresse https://softwaresupport.softwaregrp.com/

Conditions préalables pour lire la documentation de Data Protector

Pour pouvoir lire les guides de Data Protector et l'aide de Data Protector, vous devez installer un visualiseur de documents PDF et un navigateur internet pris en charge. Vous trouverez ci-dessous une liste des applications et des versions prises en charge. Micro Focus recommande l'utilisation de la dernière version disponible pour votre système d'exploitation :

- Il vous faut Adobe Reader pour pouvoir lire les guide. Les versions suivantes sont prises en charge :

  Systèmes Windows, Solaris et Linux :

  - Adobe Reader 9 ou plus récent

    Vous pouvez l'obtenir ici : http://get.adobe.com/reader/.

  Systèmes HP-UX :

  - Adobe Reader 7 ou plus récent

    Vous pouvez l'obtenir ici : ftp://ftp.adobe.com/pub/adobe/reader/unis/7x/7.0.9/enu/.

  Les autres visualiseurs de documents PDF peuvent convenir, mais n'ont pas été testés.
- Pour lire l'aide, il vous faut un navigateur internet capable d'utiliser le même processus que l'interface graphique de Data Protector sous le même compte. JavaScript doit être activé. Les navigateurs suivants sont pris en charge :

  Systèmes Windows :

  - Windows Internet Explorer 8.0 ou plus récent [1]

    Il est conseillé de désactiver l'affichage de compatibilité pour les sites web hébergés en local.

[1] Il s'agit également d'une condition préalable pour lire l'aide de l'Extension de restauration granulaire Data Protector pour Microsoft Exchange Server.

Vous pouvez télécharger Windows Internet Explorer à cette adresse : http://windows.microsoft.com/en-us/internet-explorer/download-ie.

- Mozilla Firefox 17.0.5 (Extended Support Release) ou plus récent

  Vous pouvez le télécharger ici : http://www.mozilla.org/en-US/firefox/organizations/all.html.

Les autres navigateurs internet peuvent convenir, mais n'ont pas été testés.

Aide

Vous pouvez accéder à l'Aide depuis la racine de n'importe quel package d'installation (zip/tar) sans avoir besoin d'installer Data Protector :

Systèmes Windows : Ouvrir `DP_help.chm`.

Systèmes UNIX : Décompressez le fichier tar `DP_help.tar.gz` et `DP_help.htm`.

Plan de la documentation

Le tableau suivant indique où trouver différents types d'informations. Les carrés grisés constituent un endroit utile à regarder en premier.

											Guide d'intégration					Guide ZDB		Guide GRE		
	Admin	Aide	Démarrage	Concepts	Installer	Dépannage	Récupération après sinistre (DR)	Interface de ligne de commande	PA	Intégration VSS	MSFT	Oracle/SAP	IBM	Sybase/NDMP	Environnement virtuel	ZDB Admin	ZDB IG	Exchange	SharePoint	Vmware
Tâches d'administration	X	X								X	X	X	X	X	X	X	X			
Sauvegarde		X	X	X						X	X	X	X	X	X	X	X			
Interface de ligne de commande								X												
Concepts, techniques		X		X						X	X	X	X	X	X	X	X	X	X	X
Récupération après sinistre				X			X													
Installation, mise à niveau			X		X				X											
Restauration instantanée				X	X											X	X			
Attribution de licences					X				X											
Limites		X			X	X			X	X	X	X	X	X	X		X			
Nouvelles fonctionnalités		X							X											
Planification de stratégie		X		X																
Procédures, tâches	X	X			X	X	X			X	X	X	X	X	X	X	X	X	X	X
Recommandations				X					X											
Conditions préalables					X				X	X	X	X	X	X	X					
Restaurer	X	X	X	X						X	X	X	X	X	X	X	X	X	X	X
Configurations prises en charge				X																
Dépannage		X			X	X				X	X	X	X	X	X	X	X	X	X	X

Abréviations

Les abréviations figurant sur la carte de la documentation sont expliquées ci-dessous. Les titres des éléments de documentation sont tous précédés par les termes "Data Protector."

Abréviation	Elément de documentation	
Admin	Guide de l'administrateur	Ce guide décrit les tâches d'administration de Data Protector.
Interface de ligne de commande	Référence à l'interface de ligne de commande	Ce guide décrit l'interface de ligne de commande et les options de commande Data Protector ainsi que leur utilisation, et fournit quelques exemples élémentaires de lignes de commande.
Concepts	Guide conceptuel	Ce guide décrit les concepts Data Protector, les concepts ZDB (sauvegarde avec temps d'indisponibilité nul), et fournit des informations contextuelles sur le fonctionnement de Data Protector. Il est destiné à être utilisé avec l'aide orientée tâche.
Récupération après sinistre (DR)	Guide de récupération après sinistre	Ce guide explique comment planifier, préparer, tester et effectuer une récupération d'urgence.
Démarrage	Guide de démarrage	Ce guide contient des informations pour vous permettre de commencer à utiliser Data Protector. Il énumère les conditions préalables d'installation, fournit des instructions sur l'installation et la configuration d'un environnement de sauvegarde de base, ainsi que les procédures pour effectuer une sauvegarde et restauration. Il énumère également les ressources pour plus d'informations.
Guide GRE	Guide de l'utilisateur Granular Recovery Extension pour Microsoft SharePoint Server, Exchange et VMware	Ce guide décrit comment configurer et utiliser l'extension de restauration granulaire Data Protector pour : • Serveur Microsoft SharePoint • Exchange Server • VMware vSphere
Aide	Aide	
Installer	Guide d'installation	Ce guide décrit comment installer le logiciel Data Protector, en prenant en

Abréviation	Elément de documentation	
		compte le système d'exploitation et l'architecture de votre environnement. Ce guide explique comment mettre à niveau Data Protector et obtenir les licences appropriées pour votre environnement.
Guide d'intégration	Guide d'intégration	Ce guide décrit les intégrations de Data Protector avec les applications suivantes : • **MSFT :** Microsoft SQL Server, Microsoft SharePoint Server, et Microsoft Exchange Server. • **IBM :** Informix Server, IBM DB2 UDB, et Lotus Notes/Domino Server. • **Oracle/SAP :** Oracle Server, SAP R3, SAP MaxDB et SAP HANA Appliance. • **Sybase/NDMP :** Sybase et Network Data Management Protocol Server. • **Environnement virtuel :** Intégration des environnements de virtualisation avec VMware vSphere, VMware vCloud Director, Microsoft Hyper-V et Citrix XenServer.
Intégration VSS	Guide d'intégration pour Microsoft VSS	Ce guide décrit les intégrations de Data Protector avec Microsoft Volume Shadow Copy Service (VSS).
PA	Annonces sur les produits, notes sur les logiciels et références	Ce guide donne une description des nouvelles fonctionnalités de la dernière version. Il fournit également des informations sur les conditions d'installation, les correctifs nécessaires et les limites, ainsi que sur les problèmes connus et les solutions de contournement.
Dépannage	Guide de dépannage	Ce guide décrit comment résoudre les problèmes que vous rencontrez lors de l'utilisation de Data Protector.
ZDB Admin	Guide de l'administrateur	Ce guide décrit comment configurer et

Abréviation	Elément de documentation	
	ZDB	utiliser l'intégration de Data Protector avec Solutions P4000 SAN, Famille de baies de disques P6000 EVA, Famille de baies de disque P9000 XP, 3PAR StoreServ Storage, NetApp Storage, EMC Symmetrix Remote Data Facility et TimeFinder. Il s'adresse aux administrateurs ou opérateurs de sauvegarde. Il couvre la sauvegarde avec temps d'indisponibilité nul, la récupération instantanée et la restauration de systèmes de fichiers et d'images de disque.
ZDB IG	Guide d'intégration ZDB	Ce guide décrit comment configurer et utiliser Data Protector pour effectuer une sauvegarde avec temps d'arrêt, une restauration instantanée et une restauration standard de bases de données Oracle Server, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server et d'un environnement virtuel pour VMware.

Intégrations

Intégrations d'applications logicielles

Application logicielle	Guides
IBM DB2 UDB	Guide d'intégration
Serveur Informix	Guide d'intégration
Serveur Lotus Notes/Domino	Guide d'intégration
Microsoft Exchange Server	Guide d'intégration, ZDB IG, Guide GRE
Microsoft Hyper-V	Guide d'intégration
Serveur Microsoft SharePoint	Guide d'intégration, ZDB IG, Guide GRE
Microsoft SQL Server	Guide d'intégration, ZDB IG

Application logicielle	Guides
Microsoft Volume Shadow Copy Service (VSS)	Intégration VSS
Serveur NDMP (Network Data Management Protocol)	Guide d'intégration
Serveur Oracle	Guide d'intégration, ZDB IG
Appliance SAP HANA	Guide d'intégration
SAP MaxDB	Guide d'intégration
SAP R/3	Guide d'intégration, ZDB IG
Serveur Sybase	Guide d'intégration
VMware vCloud Director	Guide d'intégration
VMware vSphere	Guide d'intégration, ZDB IG, Guide GRE

Intégrations système baie de disques

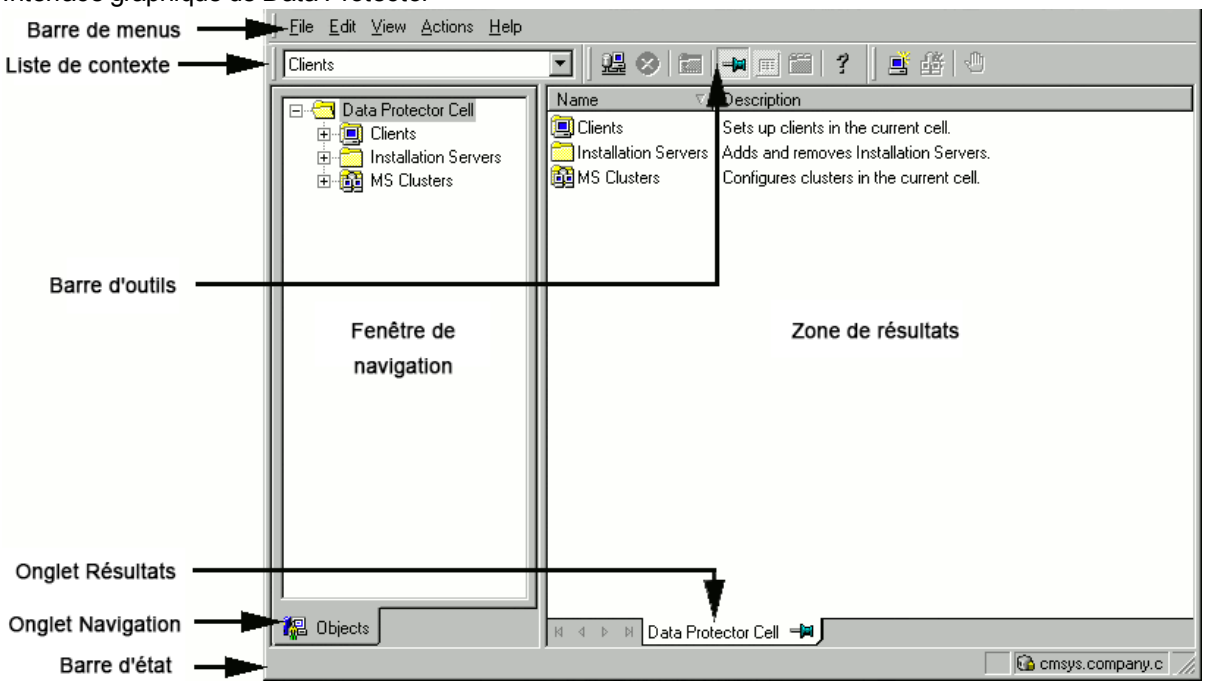
Rechercher dans ces guides pour plus de détails sur les intégrations avec les familles suivantes de systèmes de baies de disques :

Famille de baies de disque	Guides
EMC Symmetrix	tout ZDB
Solutions P4000 SAN	Concepts, ZDB admin, Guide d'intégration
Famille de baies de disques P6000 EVA	Tous ZDB, Guide d'intégration
Famille de baies de disque P9000 XP	Tous ZDB, Guide d'intégration
3PAR StoreServ Storage	Concepts, ZDB admin, Guide d'intégration
Stockage NetApp	tout ZDB

Interface graphique de Data Protector

Data Protector propose une interface graphique pour les systèmes d'exploitation Windows. Pour plus d'informations, consultez l'*Aide de Data Protector*.

Interface graphique de Data Protector



Envoyez vos commentaires sur la documentation

Pour soumettre vos commentaires relatifs à ce document, vous pouvez contacter l'équipe de documentation par e-mail. Si un client de messagerie est configuré sur ce système, cliquez sur le lien ci-dessus pour accéder à une fenêtre contenant le libellé suivant sur la ligne Objet :

Remarques concernant Guide d'installation (Data Protector 10.00)

Ajoutez simplement vos commentaires dans l'e-mail et cliquez sur **Envoyer**.

Si aucun client de messagerie électronique n'est disponible, copiez les informations ci-dessous dans un nouveau message dans un client de messagerie électronique Web, et envoyez vos commentaires à docs.feedback@microfocus.com.

Nous sommes heureux de recevoir vos commentaires !