Hewlett Packard
Enterprise

HPE Data Protector

Version du logiciel : 10.00

Guide de l'administrateur

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 Hewlett Packard Enterprise Development LP 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. HPE 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 HPE 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.hpe.com/patches.

Pour vérifier que vous disposez de l'édition la plus récente d'un document, accédez à la page : https://softwaresupport.hpe.com/manuals.

Pour accéder à ce site, vous devez créer un compte HPE Passport et vous connecter. Pour obtenir un identifiant HPE Passport, accédez à l'adresse : https://hpp12.passport.hpe.com/hppcf/login.do.

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

Support

Visitez le site d'assistance HPESoftware à l'adresse : https://softwaresupport.hpe.com

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

L'assistance en ligne de HPE 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 HPE
- 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 HPE Passport et vous identifier comme tel. De nombreuses offres nécessitent en outre un contrat d'assistance.

Pour obtenir un identifiant HPE Passport, accédez à l'adresse https://hpp12.passport.hpe.com/hppcf/login.do.

Pour plus d'informations sur les niveaux d'accès, accédez à la page https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

Sommaire

Chapitre 1: Introduction

A propos de Data Protector

HPE Data Protector est une solution de sauvegarde qui offre une protection fiable des informations et une grande facilité d'accès aux données de votre entreprise dont le volume augmente rapidement. Data Protector procure une fonctionnalité complète de sauvegarde et de restauration spécialement conçue pour les environnements intra-entreprise et les environnements partagés.

Principales fonctionnalités de Data Protector

- Architecture évolutive et d'une grande flexibilité
- Prise en charge des environnements mixtes
- Administration facile et centralisée
- Fonction de sauvegarde haute performance
- Procédure de restauration facile
- Sécurité des communications de données et de contrôle
- Grande disponibilité des données
- Opération automatisée ou sans surveillance
- Surveillance, rapports et notifications
- Gestion des services
- Intégration avec les applications de base de données en ligne
- Intégration avec d'autres produits

Architecture de HPE Data Protector

Data Protector peut être utilisé dans des environnements allant d'un simple système à des milliers de systèmes répartis sur plusieurs sites. L'unité de gestion de base est la cellule Data Protector.

La cellule Data Protector est un environnement réseau doté d'un système de Gestionnaire de cellule, d'un ou plusieurs serveurs d'installation, de systèmes client et de périphériques.

Vous pouvez installer le Gestionnaire de cellule et le serveur d'installation sur le même système (option par défaut) ou sur des systèmes séparés.

Gestionnaire de cellule

Le Gestionnaire de cellule est le système principal qui contrôle la cellule Data Protector depuis un point central, sur lequel est installé le logiciel Data Protector avec l'IDB (base de données interne). Il exécute des Gestionnaires de session, qui contrôlent les sessions de sauvegarde et de restauration, et inscrivent les informations de session dans l'IDB. L'IDB assure le suivi des fichiers sauvegardés ainsi que de la configuration de la cellule Data Protector.

Serveur d'installation

Le serveur d'installation est l'ordinateur qui héberge le référentiel du Data Protector logiciel . Vous devez avoir au moins un serveur d'installation pour UNIX et un pour l'environnement Windows afin de pouvoir effectuer des installations à distance via le réseau et distribuer les composants logiciels aux systèmes client dans la cellule.

Systèmes client

Après avoir installé le logiciel Data Protector sur le système du Gestionnaire de cellule, vous pouvez installer les composants Data Protector sur chaque système de la cellule. Ces systèmes deviennent des clients Data Protector. Le rôle d'un client dépend du logiciel Data Protector installé sur ce système.

Systèmes à sauvegarder

L'Agent de disque Data Protector (également appelé Agent de sauvegarde) doit être installé sur les systèmes client que vous souhaitez sauvegarder. L'Agent de disque lit ou écrit des données à partir d'un disque sur le système et envoie ou reçoit des données d'un Agent de support. L'Agent de disque est également installé sur le Gestionnaire de cellule, ce qui vous permet de sauvegarder des données sur le Gestionnaire de cellule, la configuration Data Protector et l'IDB (base de données interne).

Systèmes dotés de périphériques de sauvegarde

L'Agent de support (MA) Data Protector doit être installé sur les systèmes client auxquels sont connectés les périphériques de sauvegarde. L'Agent de support lit ou écrit des données à partir d'un support du périphérique et envoie des données à l'Agent de disque ou en reçoit de ce dernier. Un périphérique de sauvegarde peut être connecté à tout système et pas uniquement au Gestionnaire de cellule. Ces systèmes client sont également appelés serveurs de lecteurs. Un système client doté de plusieurs périphériques de sauvegarde est appelé serveur de lecteurs multiples.

Présentation des tâches nécessaires à la configuration de HPE Data Protector

La configuration de Data Protector est facile, mais une planification avancée permet de personnaliser l'environnement et d'optimiser les sauvegardes. Vous trouverez dans cette section un aperçu général des tâches à effectuer pour configurer un environnement de sauvegarde.

Suivant la taille et la complexité de votre environnement, toutes ces étapes ne sont pas obligatoires.

Procédure

1. Analysez la structure de votre réseau et de votre organisation. Déterminez les systèmes qui devront être sauvegardés. Pour plus d'informations, voir *Guide conceptuel HPE Data Protector*.
2. Déterminez si vous souhaitez sauvegarder des applications et des bases de données

particulières, telles que Microsoft Exchange Server, Microsoft SQL Server, Oracle Server, SAP R/3, ou autres. Data Protector fournit des intégrations spécifiques à ces produits.

Pour plus d'informations sur la configuration des intégrations, consultez le *Guide d'intégration HPE Data Protector*.

3. Choisissez la configuration de votreData Protector cellule, comme :
   - Le système qui vous servira de Gestionnaire de cellule
   - Les systèmes sur lesquels sera installée l'interface utilisateur
   - Une sauvegarde locale ou une sauvegarde réseau
   - Les systèmes qui contrôleront vos périphériques de sauvegarde et bibliothèques
   - Le type de connexion (LAN et/ou SAN)
4. Achetez les licences Data Protector requises pour votre configuration. Vous pourrez ainsi obtenir les mots de passe nécessaires à l'installation.

   Vous pouvez également utiliser Data Protector à l'aide d'un mot de passe instantané. Celui-ci n'est cependant valable que pendant 60 jours à compter de la date d'installation. Voir *Guide d'installation HPE Data Protector*.
5. Pensez aux aspects de sécurité :
   - Analysez les exigences de sécurité. Voir *Guide d'installation HPE Data Protector*.
   - Définissez les groupes d'utilisateurs que vous devez configurer.
   - Améliorez la sécurité en écrivant des données vers les supports au format crypté.
6. Choisissez une structure pour vos sauvegardes :
   - De quels pools de supports aimeriez-vous disposer, et comment seront-ils utilisés ?
   - Quels périphériques seront utilisés, et comment ?
   - Combien de copies de chaque sauvegarde voulez-vous ?
   - Combien de spécifications de sauvegarde souhaitez-vous, et comment devraient-elles être regroupées ?
   - Si vous comptez sauvegarder votre disque, pensez à des stratégies avancées, telles qu'une sauvegarde synthétique ou un Disk Staging.
7. Installez le Gestionnaire de cellule Data Protector et le(s) serveur(s) d'installation. Puis utilisez l'interface utilisateur Data Protector pour distribuer les agents Data Protector aux autres systèmes. Pour plus d'informations, voir *Guide d'installation HPE Data Protector*.
8. Configurez les périphériques de sauvegarde.
9. Configurez les pools de supports et préparez les supports.
10. Configurez les spécifications de sauvegarde, notamment la sauvegarde de l'IDB.
11. Le cas échéant, configurez les rapports.

12. Préparez la récupération après sinistre. Pour plus d'informations sur la récupération après sinistre, reportez-vous au *Guide de récupération après sinistre HPE Data Protector.*
13. Familiarisez-vous avec des tâches telles que :
    - Gestion des sauvegardes ayant échoué
    - Restaurations
    - Duplication des données sauvegardées et mise au coffre des supports
    - Test de la récupération après sinistre
    - Maintenance de l'IDB

Fonctionnement de HPE Data Protector

Les tâches de sauvegarde et de restauration sont effectuées pendant les sessions. Plusieurs sessions peuvent être exécutées simultanément. Le nombre de sessions est limité par les ressources de la cellule, comme la configuration du Gestionnaire de cellule (vitesse du processeur, taille de la mémoire principale, espace disque).

Session de sauvegarde

Une session de sauvegarde est un processus consistant à sauvegarder les données d'un système client sur des supports. Ce processus s'exécute toujours sur le système du Gestionnaire de cellule. Une session de sauvegarde est basée sur une spécification de sauvegarde et démarrée de manière interactive par un opérateur ou sans surveillance à l'aide du Planificateur Data Protector.

Session de restauration

Une session de restauration est un processus consistant à restaurer vers un disque des données préalablement sauvegardées. La session de restauration est interactive et démarrée par un opérateur à l'aide de l'interface utilisateur Data Protector.

Commandes pré-exécution et post-exécution

Les commandes de pré-exécution permettent d'effectuer certaines actions avant une session de sauvegarde ou de restauration. Les commandes de post-exécution permettent d'effectuer certaines actions après une session de sauvegarde ou de restauration.

Les commandes pré- et post-exécution peuvent être soit définies pour une spécification de sauvegarde et, à ce titre, exécutées sur le système du Gestionnaire de cellule, soit spécifiées comme option d'objet sauvegarde et exécutées sur le système client où est lancé l'Agent de disque correspondant.

Les commandes de script pré- et post-exécution peuvent être écrites sous forme d'exécutables ou de fichiers de commandes (sous des systèmes Windows) ou de scripts shell (sous des systèmes UNIX). Elles ne sont pas fournies par Data Protector et doivent être écrites séparément (par l'opérateur de sauvegarde, par exemple).

Sessions de copie d'objets, de consolidation d'objet et de vérification d'objet

Une session de copie d'objets est définie par une spécification de copie d'objets. Une session de consolidation d'objets est définie par une spécification de consolidation d'objets. Les deux types de sessions peuvent être démarrés de manière interactive ou automatique.

Une session de vérification d'objets est définie par une spécification de vérification d'objets. Celle-ci vérifie l'intégrité de données des objets créés par les sessions de sauvegarde, de copie d'objets ou de consolidation d'objet, ainsi que la capacité à les remettre à l'emplacement requis. Les sessions peuvent être démarrées de manière interactive ou automatique.

Interfaces utilisateur

Data Protector fournit une interface utilisateur graphique (GUI) et une interface de ligne de commande (CLI).

Interface utilisateur graphique

L'interface utilisateur graphique est fournie pour les systèmes Windows.

Via l'interface utilisateur graphique, Data Protector vous permet de gérer l'intégralité de votre environnement de sauvegarde à partir d'un seul système. Vous pouvez même gérer plusieurs environnements de sauvegarde à partir d'un seul système. L'architecture Data Protector vous offre la flexibilité d'installer et d'utiliser l'interface utilisateur Data Protector. L'interface utilisateur n'a pas besoin d'être utilisée à partir du système Gestionnaire de cellule ; vous pouvez l'installer sur votre système de bureau.

Pour faciliter son utilisation, l'interface utilisateur peut être installée sur différents systèmes, permettant à plusieurs administrateurs d'accéder à Data Protector via leurs consoles installées localement. Avant de pouvoir commencer à utiliser l'interface utilisateur Data Protector sur le système client, ajoutez un utilisateur de ce système à un groupe d'utilisateurs Data Protector sur le Gestionnaire de cellules.

Une installation et une configuration spécifiques sont nécessaires pour afficher les caractères internationaux dans les noms de fichiers et les messages de sessions.

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

Interface en ligne de commande

Outre l'interface utilisateur graphique, une interface de ligne de commande est disponible sur les systèmes Windows et UNIX. L'interface de ligne de commande (CLI) respecte le format standard UNIX pour les commandes et les options, offrant ainsi une fonctionnalité Data Protector complète. Vous pouvez utiliser ces commandes dans des scripts afin d'accélérer vos tâches courantes.

La page du manuel `omniintro` répertorie toutes les commandes Data Protector prises en charge et précise les différences entre les commandes sur les plates-formes UNIX et Windows. Pour plus d'informations, voir *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Personnalisation des paramètres de langue dans l'interface utilisateur

La manipulation des noms de fichier dans un environnement hétérogène (systèmes d'exploitation et paramètres régionaux différents dans une même cellule) peut se révéler très complexe. Une configuration particulière est nécessaire pour pouvoir afficher correctement les noms des fichiers qui ont été sauvegardés avec des paramètres régionaux donnés, puis consultés ou restaurés avec d'autres paramètres régionaux.

Conditions préalables

Les conditions préalables suivantes s'appliquent au système avec interface utilisateur :

- Installez les polices appropriées au jeu de caractères codés sélectionné dans l'interface utilisateur Data Protector. Par exemple, pour utiliser les caractères japonais dans l'interface utilisateur d'un système européen, installez les polices japonaises.

Limites

- La mise en œuvre de la conversion d'encodage de caractères sous Windows diffère légèrement de la mise en œuvre sous UNIX. Le mappage de certains caractères peut ne pas s'effectuer correctement si l'interface utilisateur Data Protector est exécutée sur une plate-forme différente de celle du client en cours de configuration. Toutefois, seuls quelques caractères ne s'afficheraient alors pas correctement, ce qui n'affectera pas les sauvegardes ou les restaurations.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**, **Moniteur**, **Restaurer**, **Rapports**, ou **Base de données interne**.
2. Dans le menu Affichage, cliquez sur **Codage**.
3. Sélectionnez le codage de caractères qui a été utilisé sur le système sur lequel les fichiers sauvegardés ont été créés.

Démarrage de l'interface utilisateur HPE Data Protector

Pour lancer l'interface Data Protector sous Windows, cliquez sur :

Démarrer > **Programmes** > **HPE Data Protector** > **Gestionnaire Data Protector**

Vous pouvez également exécuter la commande `manager`.

Pour indiquer le Gestionnaire de cellule auquel vous voulez vous connecter, exécutez la commande suivante :

`manager -server Cell_ Manager_name`.

Des options spécifiques du contexte de cette commande permettent de lancer un ou plusieurs contextes Data Protector. Pour lancer les contextes de sauvegarde et de restauration Data Protector, exécutez la commande suivante :

```
manager -backup -restore
```

Pour plus d'informations sur ces commandes, reportez-vous à la page de manuel `omnigui` ou à la *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Utilisation de la console Microsoft Management Console (MMC)

Sous les systèmes Windows, vous pouvez utiliser la Console de gestion Microsoft pour accéder à la page d'accueil Data Protector ou lancer l'interface utilisateur Data Protector.

Le composant logiciel enfichable Data Protector `OB2_Snap` fournit une intégration de base de Data Protector et de la console. Pour l'utiliser, procédez comme suit :

Procédure

1. Dans le groupe de programmes Data Protector, sélectionnez le **composant logiciel enfichable Data Protector**.
2. Au niveau de la racine de la console, sélectionnez **HPE Data Protector** pour afficher les options disponibles.

Lancement de HPE Storage Optimizer à partir de l'interface utilisateur graphique de Data Protector

Vous pouvez lancer HPE Storage Optimizer à partir de la GUI de Data Protector en réalisant les étapes suivantes :

1. Ajoutez la variable `StorageOptServer` dans le fichier Data Protector **Global**.

   Elle doit être dans le format suivant : `StorageOptServer = <server name>`. Cette étape est obligatoire.
2. Dans le contexte de sauvegarde, naviguez vers **Actions** > **HPE Storage Optimizer**. Storage Optimizer s'ouvre dans une nouvelle fenêtre du navigateur web.

Chapitre 2: Tâches de configuration

Sécurité système

Dans Data Protector 10.00 toutes les communications ont lieu par défaut via TLS 1.2. Pour configurer la confiance entre le client et le Gestionnaire de cellule, certaines conditions doivent être satisfaites avant l'installation. Avant la version 10.00 de Data Protector, les clients avaient la possibilité de sécuriser la communication entre le Gestionnaire de cellule et le client en activant ECC (Encrypted Control Communication). Les clients DA et MA ECC antérieurs à la version 10.00 peuvent continuer à utiliser Data Protector 10.00.

Dans la version 10.00, toutes les commandes et l'exécution des scripts sont acheminées via le Gestionnaire de cellule. L'execution centralisee des commandes fait en sorte que les controles, comme les donnees, sont envoyes sur un canal TLS securise, ce qui garantit l'integrite des donnees. De plus, les clients Data Protector à présent écoutent et acceptent uniquement les instructions et l'exécution de la commande de script d'un Gestionnaire de cellule approuvé et vérifié, ce qui réduit significativement le risque de violations de la sécurité.

Pour plus de détails sur la sécurité, consultez le *Guide d'installation HP Data Protector*.

Configurer des certificats pour la communication sécurisée

Au cours de l'installation, les certificats auto-signés basés sur OpenSSL sont utilisés pour établir la confiance pour la communication sécurisée avec la vérification par empreinte. Si vous le souhaitez, vous pouvez remplacer les certificats OpenSSL générés pendant l'installation de Data Protector par des certificats personnalisés après l'installation de Data Protector. Les procédures qui suivent décrivent comment générer des certificats personnalisés, régénérer les certificats et les redistribuer.

Générer des certificats personnalisés

L'utilisateur peut générer un certificat personnalisé et copier le fichier vers les chemins d'accès suivants :

Windows :

Clé privée : `<DP_HOME>\config\sscertificates\localhost_key.pem`

Certificat auto-signé : `<DP_HOME>\config\sscertificates\localhost_cert.pem`

UNIX :

Clé privée : `/etc/opt/omni/config/sscertificates/localhost_key.pem`

Certificat auto-signé : `/etc/opt/omni/config/sscertificates/localhost_cert.pem`

Régénération de certificats dans Data Protector

Exécutez la commande suivante pour régénérer un certificat dans Data Protector :

```
omnicc -secure_comm -regenerate_cert
```

Redistribuer des certificats

La redistribution de certificats doit être effectuée pendant l'utilisation de certificats personnalisés ou si les certificats doivent être régénérés.

Redistribuer un certificat Gestionnaire de cellule

1. Reconfigurez le certificat Gestionnaire de cellule dans tous les serveurs Serveur d'installation (Windows et Unix compris) en exécutant la commande suivante :

   ```
   omnicc -secure_comm -reconfigure_peer <CM hostname>
   ```

2. Pour redistribuer et reconfigurer, la commande suivante doit être exécutée sur le GC :

   ```
   omnicc -secure_comm -reconfigure_peer_all <input_file_path>
   ```

   Le paramètre `<input_file_path>` est optionnel. Ce fichier doit disposer des informations d'identification de tous les clients faisant partie de la cellule.

   Le format du fichier est :

   ```
   -host "linux_client_hostname" -user "<username>" -pass "password"
   -host "windows_client_hostname" -user "<Domain>\<username>" -pass "<password>"
   ```

   Chaque rang correspond ici à un client, et le nom d'utilisateur et le mot de passe doivent être mentionnés comme décrit ci-dessus.

   Si le `<input_file_path>` n'est pas spécifié, `omnicc` demande les informations d'identification des clients alors qu'il tente de redistribuer et de reconfigurer le certificat Gestionnaire de cellule.

   > **REMARQUE :**
   > Le nom `Domain` doit comporter un préfixe pour les clients Windows.

Redistribuer un certificat de client

Si un certificat de client est généré, il doit être redistribué au Gestionnaire de cellule. Exécutez la commande suivante :

```
omnicc -secure_comm -reconfigure_peer <client_host_name>
```

Rapports

La notification **WarnCertificateExpiry** est ajoutée à la section Notifications dans le contexte de génération de rapports.

Avec ceci, l'utilisateur peut générer une notification pour les certificats sur le point d'expirer.

Par défaut, les notifications sont générées pour les certificats sur le point d'expirer dans 7 jours. Des notifications anticipées peuvent être générées en changeant la valeur de la variable globale **WarnCertificateExpiryBefore**.

Connexion à une interface utilisateur Gestionnaire de cellule/Jumpstation à partir de l'interface utilisateur graphique

En cas d'utilisation d'un hôte sur lequel le composant Console de cellule est installé pour établir la connexion à plusieurs gestionnaires de cellule, l'hôte sur lequel le composant CC est installé doit être

sécurisé avec tous les gestionnaires de cellule auxquels il est destiné à se connecter et tous les GC doivent être sécurisés avec l'hôte de l'interface graphique.

Par exemple :

Cas 1 :

Si hostX est utilisé pour se connecter aux instances Gestionnaire de cellule hostCM1, hostCM2 et hostCM3 (tous étant de version 10.0 ou supérieure), exécutez les commandes suivantes sur hostX :

```
Omnicc –secure_comm –configure_peer <hostCM1>
```

```
Omnicc –secure_comm –configure_peer <hostCM2>
```

```
Omnicc –secure_comm –configure_peer <hostCM3>
```

Exécutez la commande suivante sur toutes les instances de Gestionnaire de cellule mentionnées ci-dessus :

```
Omnicc –secure_comm –configure_peer <hostX>
```

Cas 2 :

Si la version de hostX est antérieure à 10.00 et que les hôtes hostCM1, hostCM2 et hostCM3 sont de version 10.0 ou supérieure, exécutez les commandes suivantes sur les trois instances de Gestionnaire de cellule :

```
Omnicc –secure_comm –configure_for_gui <hostX>
```

Cas 3 :

Si les instances de CM sont antérieures à la version 10.0 et que hostX est de version 10.0 ou supériieure, exécutez la commande suivante sur hostX :

```
Omnicc –secure_comm –configure_for_gui <hostCM1>
```

```
Omnicc –secure_comm –configure_for_gui <hostCM2>
```

```
Omnicc –secure_comm –configure_for_gui <hostCM3>
```

Cas 4 :

Si hostCM1 est antérieur à la version 10.0 et que hostCM2, hostCM3 et hostX sont de version 10.0 ou supérieure, Exécutez la commande suivante sur hostX :

```
Omnicc –secure_comm –configure_for_gui <hostCM1>
```

```
Omnicc –secure_comm –configure_peer <hostCM2>
```

```
Omnicc –secure_comm –configure_peer <hostCM3>
```

Exécutez la commande suivante sur hostCM2 et hostCM2

```
Omnicc –secure_comm –configure_peer <hostX>
```

Sécurité des utilisateurs

Les utilisateurs de Data Protector constituent l'un des niveaux de sécurité essentiels de Data Protector. La configuration des utilisateurs doit être préparée et testée avec soin.

Droits utilisateur

Certains utilisateurs sont très puissants et représentent donc un risque pour la sécurité. Par exemple, les droits d'utilisateur de la configuration utilisateur et de la configuration clients pemettent à un utilisateur de modifier les paramètres de sécurité.

Le droit utilisateur **Restaurer vers d'autres clients** est également très puissant, en particulier s'il est associé au droit utilisateur **Sauvegarder en tant que root** ou **Restaurer en tant que 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.

Droit utilisateur Démarrer spécification de sauvegarde

L'utilisateur est autorisé à démarrer les sessions de sauvegarde pour une spécification de sauvegarde à partir de la ligne de commande en utilisant le `omnib` avec l'option `-datalist`.

En associant les droits utilisateur **Démarrer spécification de sauvegarde** et **Démarrer la sauvegarde**, un utilisateur est autorisé à afficher les spécifications de sauvegarde configurées dans l'interface utilisateur et il peut démarrer une session de sauvegarde pour une spécification de sauvegarde ou une sauvegarde interactive

Autoriser les utilisateurs à effectuer des sauvegardes interactives n'est pas toujours souhaitable. Pour permettre des sauvegardes interactives uniquement vers les utilisateurs qui ont également le droit d'utilisateur **Sauvegarder la spécification de sauvegarde**, définissez l'option globale `StrictSecurityFlags` à `0x0200`.

Masquage du contenu des spécifications de sauvegarde

Dans un environnement à sécurité élevée, le contenu des spécifications de sauvegarde enregistrées peut être considéré comme sensible ou même confidentiel.

Data Protector peut être configuré pour masquer le contenu des spécifications de sauvegarde pour tous les utilisateurs, sauf pour ceux disposant du droit utilisateur **Save backup specification**. Pour cela, définissez l'option globale `StrictSecurityFlags` sur `0x0400`.

Groupements d'hôtes approuvés

La fonctionnalité de groupement d'hôtes approuvés réduit la nécessité d'accorder le droit utilisateur **Restaurer vers d'autres clients** à des utilisateurs lorsque ceux-ci n'ont besoin que de restaurer des 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.

Groupes d'utilisateurs

Data Protector n'a, par défaut, que 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.

Restrictions utilisateur

En plus de la définition de groupes d'utilisateurs spécifiques, vous pouvez aussi restreindre les actions utilisateur à exécuter à quelques systèmes de la cellule uniquement. Vous pouvez renforcer ces restrictions en configurant le fichier `user_ restrictions` sur le Responsable de Cellule. Les restrictions s'appliquent uniquement aux membres des groupes d'utilisateurs Data Protector autres que admin et opérateur.

Validation utilisateur

La configuration des utilisateurs est liée à la validation utilisateur. 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 qu'il n'y ait aucune spécification utilisateur "faible" dans la liste des utilisateurs Data Protector. Notez que la partie client d'une spécification utilisateur est la partie forte (en particulier avec la validation optimisée), alors que les parties utilisateur et le groupe ne peuvent pas être vérifiées de façon 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 des clients multiples sont utilisés, une entrée doit être ajoutée pour chaque client, plus qu'indiquer cet utilisateur comme `user`, `group`, `<Any>`. Les utilisateurs non fiables ne doivent pas être autorisés à se connecter à l'un de ces systèmes.

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. Pour activer la vérification stricte du nom d'hôte, définissez l'option globale `StrictSecurityFlags`sur `0x0001`.

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 mise en œuvre 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 un 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 ce paramètre.

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 les éléments suivants :

- Agent d'application (OB2BAR) sur les clients Windows. Il faut ajouter l'utilisateur `SYSTEM`, `NT AUTHORITY`,*`client`* à 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, le compte doit déjà avoir été paramétré.

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.

Le recours aux 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.

Journaux de sécurité

Si vous rencontrez des problèmes d'accès à la fonctionnalité ou aux clients Data Protector, vous pouvez utiliser les informations des fichiers journaux pour déterminer le problème. Par exemple, les événements consignés peuvent vous aider à déterminer les utilisateurs ou clients mal configurés.

Evénements de sécurité des clients

Les événements de sécurité des clients sont consignés dans le fichier `inet.log` qui réside dans le répertoire des fichiers journaux Data Protector par défaut sur chaque client dans la cellule.

Il est utilie de vérifier l'activité récente de Data Protector sur les clients.

Evénements de sécurité du Gestionnaire de cellule

Les événements de sécurité du Gestionnaire de cellule sont consignés dans le fichier `security.log` qui réside dans le répertoire des fichiers journaux du serveur Data Protector par défaut.

Le fichier `security.log` est créé avec le premier événement de sécurité.

Configuration de groupements d'hôtes approuvés

Vous pouvez définir des groupes d'hôtes qui se confieront les données.

Procédure

1. Sur un Gestionnaire de cellule Windows, créez le fichier *données_programme_Data_Protector*`\Config\Server\cell\host_trusts`.

   Sur un Gestionnaire de cellule UNIX, créez le fichier `/etc/opt/omni/server/cell/host_trusts`.
2. Répertoriez les hôtes approuvés dans ce fichier.

   Par exemple :

   ```
   GROUP="cluster.domain.com"
   {
   cluster.domain.com
   node1.domain.com
   node2.domain.com
   }
   GROUP="DFG"
   {
   computer.domain.com
   ```

```
anothercomputer.domain.com
}
```

3. Enregistrez le fichier.

Cryptage

À propos du cryptage de données

Data Protector vous permet de crypter des données sauvegardées afin de les protéger. Deux techniques de cryptage de données sont disponibles : le cryptage sur logiciel et le cryptage sur lecteur.

Le cryptage logiciel Data Protector appelé cryptage AES 256 bits, s'appuie sur l'algorithme cryptographique AES (Advanced Encryption Standard), qui utilise la même clé pour le cryptage et le décryptage. Les données sont cryptées avant d'être transférées sur le réseau et d'être écrites sur un support.

Le cryptage sur lecteur Data Protector utilise la fonctionnalité de cryptage du lecteur. La capacité réelle de mise en œuvre et de cryptage dépend du microprogramme du lecteur. Data Protector active simplement la fonctionnalité et gère les clés de cryptage.

Une fois la fonction de cryptage activée, il n'est pas nécessaire de procéder à d'autres paramétrages. Cependant, pour le cryptage AES 256 bits, Data Protector vous permet de gérer manuellement les clés de cryptage (expiration, réactivation, exportation, importation et suppression des clés) via l'interface de ligne de commande (CLI).

Les interfaces graphique et de ligne de commande de Data Protector vous permettent de déterminer quels objets sauvegarde sont cryptés ou quels supports de sauvegarde contiennent des objets cryptés, ainsi que d'obtenir des informations détaillées sur le cryptage de ces objets.

Activation du cryptage AES 256 bits

Vous pouvez activer le cryptage logiciel AES 256 bits lors de la création d'une nouvelle spécification de sauvegarde ou la modification d'une spécification de sauvegarde déjà configurée.

Conditions préalables

- Vous devez posséder une clé de cryptage active avant d'effectuer une sauvegarde cryptée de l'IDB. Pour plus d'informations, reportez-vous à la page de manuel `omnikeytool` ou à la *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Limites

- Le cryptage AES 256 bits ne crypte pas les métadonnées, comme le nom et la taille de fichier.
- Le cryptage n'est pas applicable à la sauvegarde ZDB sur disque ou la partie disque de la sauvegarde ZDB sur disque + bande.
- Les objets sauvegardés avec le cryptage AES 256 bits ne peuvent pas être consolidés.

Activation du cryptage dans une spécification de sauvegarde de système de fichiers

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis **Système de fichiers**. Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez sur la spécification de sauvegarde à modifier.
4. Dans la page de propriétés Options, cliquez sur le bouton **Avancé** pour Options du système de fichiers.
5. Dans la fenêtre Options du système de fichiers, cliquez sur l'onglet **Autre**. Dans la liste déroulante **Sécurité des données**, sélectionnez l'option **AES 256 bits**.
6. Cliquez sur **OK** puis sur **Appliquer** pour enregistrer les modifications.

> **CONSEIL :**
> Pour ne crypter que les objets sauvegarde sélectionnés, allez dans l'onglet **Résumé d'objet de sauvegarde** et sélectionnez l'option **AES 256 bits** dans les propriétés de l'objet.

Activation du cryptage dans une spécification de sauvegarde d'image de disque

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis **Système de fichiers**. Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez sur la spécification de sauvegarde à modifier.
4. Dans la page Résumé d'objet sauvegarde, cliquez sur le bouton **Propriétés**.
5. Dans la fenêtre Propriétés d'objet, cliquez sur l'onglet **Autre**. Dans la liste déroulante **Sécurité des données**, sélectionnez l'option **AES 256 bits**.
6. Cliquez sur **OK** puis sur **Appliquer** pour enregistrer les modifications.

Activation du cryptage dans une spécification de sauvegarde de base de données interne

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécifications de sauvegarde**, puis **Base de données interne**. Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez sur la spécification de sauvegarde à modifier.
4. Dans la page Options, sous Options communes de l'application, cliquez sur **Avancé**.
5. Dans la fenêtre Options communes de l'application, cliquez sur l'onglet **Autre**. Dans la liste déroulante **Sécurité des données**, sélectionnez l'option **AES 256 bits**.
6. Cliquez sur **OK** puis sur **Appliquer** pour enregistrer les modifications.

Activation du cryptage dans une spécification de sauvegarde d'intégration d'application

Limites

- Pour la liste actualisée des intégrations d'applications prenant en charge le cryptage AES 256 bits, consultez les dernières matrices de support à l'adresse https://softwaresupport.hpe.com/.
- Il n'est pas possible d'utiliser une combinaison des options **Mode Fast direct** et **AES 256 bits** pour l'intégration Microsoft SQL Server.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez Spécifications de sauvegarde, puis le type de **spécification de sauvegarde** approprié (par exemple, **MS SQL Server**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez sur la spécification de sauvegarde à modifier.
4. Dans la page de propriétés Options, cliquez sur le bouton **Avancé** pour Options communes de l'application.
5. Dans la fenêtre Options communes de l'application, cliquez sur l'onglet **Autre**. Dans la liste déroulante **Sécurité des données**, sélectionnez l'option **AES 256 bits**.
6. Cliquez sur **OK** puis sur **Appliquer** pour enregistrer les modifications.

Exportation et importation de supports avec sauvegardes cryptées

Pour restaurer des données d'une sauvegarde cryptée vers un client dans une cellule Data Protector différente, vous devez importer les supports et les clés de cryptage dans le Gestionnaire de cellule de destination conformément aux instructions suivantes.

> **REMARQUE :**
> Data Protector permet également de gérer manuellement les clés de cryptage (expiration, réactivation, exportation, importation et suppression des clés) via l'interface de ligne de commande (CLI). Pour plus d'informations, reportez-vous à la page de manuel `omnikeytool` ou à la *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Environnement Gestionnaire de cellule ou environnement MoM sans CMMDB

Dans un environnement Gestionnaire de cellule ou MoM dans lequel des MMDB locales sont utilisées, suivez les étapes ci-dessous pour exporter et importer un support avec sauvegarde cryptée :

Procédure

1. Sur le Gestionnaire de cellule d'origine, exportez le support depuis l'IDB. Cette opération exporte aussi les clés de cryptage pertinentes de la banque de clés vers le fichier *`mediumID`*`.csv`, dans le répertoire des clés de cryptage exportées par défaut.
2. Transférez le fichier *`mediumID`*`.csv` vers le Gestionnaire de cellule de destination et placez-le dans le répertoire des clés de cryptage importées par défaut.

3. Insérez le support exporté dans le lecteur qui sera utilisé par le Gestionnaire de cellule de destination.
4. Dans le Gestionnaire de cellule de destination, importez le support. Lors de cette opération, les clés sont également importées depuis le fichier *mediumID*.csv.

> **REMARQUE :**
> Si le fichier des clés est manquant, vous pouvez néanmoins importer le support, mais l'importation du catalogue ne peut pas être effectuée en raison de l'absence des clés de décryptage.

Environnement MoM avec CMMDB

Dans un environnement MoM dans lequel la CMMDB est utilisée, toutes les informations relatives aux supports sont stockées dans le Gestionnaire MoM, mais les ID des clés de cryptage utilisés par ces supports ainsi que la CDB sont stockés dans une banque de clés locale dans chaque Gestionnaire de cellule. Notez que toutes les opérations de gestion des supports doivent être réalisées dans le Gestionnaire de cellule MoM.

Pour exporter et importer un support avec sauvegarde cryptée lorsque la CMMDB réside dans le Gestionnaire MoM, procédez comme suit :

Procédure

1. Exportez le support à partir de la CMMDB Les ID des clés sont exportés vers le fichier *mediumID*.csv, dans le répertoire des clés de cryptage exportées par défaut.
2. Transférez le fichier *mediumID*.csv vers le Gestionnaire de cellule de destination et placez-le dans le répertoire des clés de cryptage importées par défaut.
3. Depuis le Gestionnaire MoM, éjectez un support d'une bibliothèque.
4. Déplacez un support du pool de supports d'origine au pool de supports de destination qui est associé à un lecteur dans la cellule de destination. Lors de cette opération, le catalogue est également importé.
5. Insérez le support exporté dans le lecteur qui sera utilisé par le Gestionnaire de cellule de destination.
6. Dans le Gestionnaire de cellule de destination, importez le support. Lors de cette opération, les clés sont également importées depuis le fichier *mediumID*.csv.

Activation du cryptage sur lecteur

Pour la liste actualisée des périphériques prenant en charge le cryptage sur lecteur, consultez les dernières matrices de prise en charge à l'adresse https://softwaresupport.hpe.com/

Vous pouvez activer le cryptage sur lecteur lors des opérations suivantes :

- Configuration d'un lecteur ou modification d'un lecteur déjà configuré
- Configuration d'une spécification de sauvegarde, de copie d'objet ou de consolidation d'objet ou modification d'une spécification de ce type déjà configurée
- Configuration d'une opération de support automatisée ou modification d'une opération de ce type déjà configurée

Conditions préalables

- Vous devez posséder une clé de cryptage active avant d'effectuer une sauvegarde cryptée de l'IDB. Pour plus d'informations, reportez-vous à la page de manuel `omnikeytool` ou à la *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Limites

- Il n'est pas possible d'utiliser le cryptage sur lecteur pour les périphériques contrôlés par serveur NDMP ou pour les lecteurs d'une bibliothèque avec un contrôle de cryptage externe (par exemple, une bibliothèque ESL sous contrôle HPE SKM).

Recommandation

- Pour optimiser les performances, utilisez une taille de bloc d'au moins 256 kilo-octets.

> **REMARQUE :**
> Lors de la sauvegarde sur un support contenant à la fois des sauvegardes cryptées et non cryptées, le message `Drive-based decryption enabled` peut s'afficher. Dans ce cas, la dernière sauvegarde sur le support est cryptée et elle est décryptée automatiquement pour que Data Protector puisse la vérifier avant l'ajout de la nouvelle sauvegarde.

Activation du cryptage sur lecteur dans la configuration du lecteur

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Périphériques** et le périphérique souhaité, puis ses lecteurs.
3. Cliquez avec le bouton droit de la souris sur le lecteur souhaité et cliquez sur **Propriétés**.
4. Dans la page de propriétés Paramètres, cliquez sur le bouton **Avancé**.
5. Dans la fenêtre Options avancées, cliquez sur l'onglet **Paramètres** et sélectionnez l'option **Cryptage sur lecteur**, puis cliquez sur **OK**.
6. Cliquez sur Appliquer pour enregistrer les modifications.

Activation du cryptage sur lecteur dans une spécification de sauvegarde

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis le type de spécification approprié (par exemple, **Système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Sélectionnez la spécification de votre choix.
4. Dans la page Destination, cliquez avec le bouton droit sur le périphérique sélectionné pour la sauvegarde et cliquez sur **Propriétés**.
5. Dans la fenêtre Propriétés du périphérique, sélectionnez l'option **Cryptage sur lecteur**, puis

cliquez sur **OK**.

6. Cliquez sur Appliquer pour enregistrer les modifications.

> **CONSEIL :**
> Pour modifier une spécification de copie d'objet ou de consolidation d'objet, ouvrez la spécification dans le contexte **Opérations sur les objets** et suivez les étapes 4 à 6.

Activation du cryptage sur lecteur pour une opération de support automatisée

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Opérations automatisées**. Toutes les opérations automatisées configurées s'affichent.
3. Cliquez sur l'opération de support pour laquelle vous souhaitez activer le cryptage sur lecteur.
4. Dans la fenêtre Options, sélectionnez l'option **Cryptage sur lecteur**, puis cliquez sur **Appliquer**.

> **REMARQUE :**
> L'option **Cryptage sur lecteur** s'applique à tous les périphériques concernés par l'opération de support automatisée.

Introduction à l'authentification utilisateur et à 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 desconnexions 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 nécessaire 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 Data 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`. Exécuter 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 cellule UNIX.

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

Pour configurer le module de connexion LDAP, utilisez la console d'administration Web de WildFly Application Server, qui est installée avec 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://nom-gestionnaire-de-cellule: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 **Connexion**. 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 préconfiguré s'affichent sur 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 :

Options 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	Un filtre de recherche permettant de localiser le contexte de l'utilisateur à authentifier

		correspondant.	
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 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` .	Le DN utilisé pour la liaison au serveur LDAP pour les requêtes 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. Exécuter 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 HPE 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 des justificatifs LDAP.

Ajouter des utilisateurs LDAP à des groupes d'utilisateurs Data Protector

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**: Sélectionnez 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 Data Protector

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**: Spécifiez 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 accorder automatiquement 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 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.
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.

Support des pare-feu

À propos du support des pare-feu

Vous pouvez configurer Data Protector dans un environnement où les processus Data Protector communiquent à travers un pare-feu. À partir de Data Protector 9.09 et 10.00, le nombre de ports qui doivent être ouverts dans le pare-feu est réduit. La modification ne se produit qu'après la mise à niveau de la cellule, et jusqu'à cette mise à niveau, les anciens clients continuent à fonctionner selon le mode hérité, et utilisent les mêmes ports que dans les versions Data Protector antérieures.

Il n'est pas nécessaire de définir les variables OB2PORTRANGE et OB2PORTRANGESPEC des ports d'écoute pour les processus Data Protector. Ces variables peuvent cependant être définies pour que Data Protector les utilise pour la communication inter processus au sein d'un hôte. Les exemples qui suivent en expliquent l'utilisation :

Exemple 1 :

HPE Data Protector 9.09 MA et version antérieure de HPE Data Protector 9.09 DA

MA ouvre un port lié à toutes les adresses. Ceci est affiché dans la sortie netstat comme MA apparaît sur le port 0.0.0.0:1234.

- "1234" est ici un exemple, en réalité, le port dépend de la plage de ports dynamiques, définie à l'aide des variables OB2PORTRANGE et de la configuration HPE Data Protector.
- "0.0.0.0" désigne "toutes adresses", et est équivalent à [::] pour l'IPv6. Cela signifie qu'un client peut se connecter par n'importe quelle voie.

Les autres processus du même hôte ne peuvent ouvrir le port 1234. DA se connecte directement à l'hôte MA 1234. Vous devez maintenir le port 1234 ouvert dans le pare-feu.

Exemple 2 :

HPE Data Protector 9.09 MA et HPE Data Protector 9.09 DA :

- Étant donné que MA ne sait pas si le DA qui se connecte est HPE Data Protector version 9.09 ou antérieure, MA maintient le port 0.0.0.0:1234 ouvert.
- Si on compare ce cas à l'exemple 1, vous n'avez pas besoin d'ouvrir le port 1234 dans le pare-feu si vous êtes sûr que seuls des clients HPE Data Protector 9.09 vont se connecter. Cela dépend de l'ordre dans lequel vous effectuez la mise à niveau des hôtes.

Exemple 3 :

HPE Data Protector 9.09 MA, HPE Data Protector 9.09 DA, et pare-feu HPE Data Protector activé sur l'hôte MA

- MA ouvre le port lié uniquement à l'interface loopback. Ceci est affiché dans la sortie netstat comme MA apparaît sur le port 127.0.0.1:1234, ou [::1]:1234 pour l'IPv6.
- Un ancien DA ne pourrait se connecter, étant donné que le port 1234 est inaccessible depuis un hôte distant, qu'il s'agisse du pare-feu Windows ou d'un autre.

> **REMARQUE :**
> Les pare-feu n'empêchent pas les processus d'ouvrir des ports, mais seulement la connexion à

ces ports depuis des hôtes distants.

Pour plus d'informations sur l'utilisation des ports dans HPE Data Protector10.00, consultez le tableau Utilisation des ports dans HPE Data Protector 9.09 et ultérieures.

Communication dans Data Protector

Les processus Data Protector communiquent à l'aide de connexions TCP/IP. Data Protector a besoin des ports suivants :

- Port Inet (5555/5565 par défaut) sur tous les systèmes Data Protector.

  REMARQUE :
  L'Inet Windows est multithread.

- Port de service IDB (7112 par défaut) sur le système du Gestionnaire de cellule.
- Port de serveur d'application (7116 par défaut) sur le système du Gestionnaire de cellule.
- La règle pour le fichier binaire StoreOnceSoftware.exe doit rester dans les exceptions entrantes de pare-feu. StoreOnceSoftware.exe ne prend pas en charge la transmission par port unique (basée sur un code tiers), mais il peut ouvrir des ports entrants et accepter les communications sur ces ports.

Ces ports doivent être ouverts dans le pare-feu (et accessibles aux hôtes distants).

De plus, Data Protector ouvre un certain nombre de ports dynamiques. Ils doivent rester ouverts dans le pare-feu jusqu'à ce que la cellule Data Protector soit mise à niveau. Une fois la cellule mise à niveau vers Data Protector 10.00 ou version ultérieure, ces ports sont utilisés au sein des processus (IPC) et ils n'ont plus besoin d'être ouverts du point de vue du pare-feu.

Les modifications suivantes sont nécessaires à la configuration de la plage de ports dynamiques :

- Limitez les morts qui doivent rester ouverts dans un pare-feu jusqu'à ce que la cellule entière soit mise à niveau.
- Empêchez Data Protector d'ouvrir des ports qui pourraient être nécessaires pour des applications tierces.
- Data Protector peut communiquer avec les logiciels non Data Protector qui pourraient avoir besoin d'ouvrir leurs propres ports.

REMARQUE :
Pendant l'installation, les ports suivants doivent être ouverts pour Inet :

- Nouvelle installation Data Protector - 5565
- Mise à niveau d'installation Data Protector - 5555

Mécanisme de configuration

Vous pouvez configurer le comportement d'allocation de ports à l'aide de deux options `omnirc` :

- OB2PORTRANGE

  Cette option définit la plage de ports depuis laquelle tous les processus Data Protector ouvrent les ports dynamiques.

- OB2PORTRANGESPEC

Avant Data Protector 10.00 et 9.09, les plages de ports remplissaient deux fonctions :

- Sécurité : limiter les ports ouverts par Data Protector, et donc les ports que l'utilisateur doit ouvrir dans le pare-feu.
- Conflits avec les autres logiciels : les logiciels non Data Protector peuvent nécessiter les ports 1000 à 2000 pour des usages spécifiques, et donc l'utilisation de OB2PORTRANGE empêche Data Protector d'utiliser cette plage de ports. Ceci est valable pour OB2PORTRANGE.

REMARQUE :
- Par défaut, les ports dynamiques sont assignés par le système d'exploitation.
- Ces options n'affectent pas les ports fixes définis pour l'Inet (5555/5565), le port de service IDB (7112), ou du serveur d'application (7116).
- Les options de plage de ports limitent l'utilisation des ports de Data Protector. Elles ne peuvent empêcher les applications autres de Data Protector d'allouer des ports sur cette plage.

Le nombre de ports ouverts dans le pare-feu est réduit lorsque les agents qui participent à la communication sont mis à niveau. Avant cette mise à niveau, Data Protector utilise l'ancienne méthode de communication. Les anciens agents de disque fonctionnent avec le nouvel agent de support, et vice-versa. L'utilisateur devrait maintenir les ports ouverts jusqu'à ce que tous les hôtes de la cellule soient mis à niveau.

Sur les plateformes où l'inet supporte l'option -p <proc_limit>, évitez si possible d'utiliser cette option. Sinon, il est recommandé d'utiliser une valeur de proc_limit supérieure à 2200.

Avant d'activer le vrai pare-feu, il est recommandé de tester Data Protector avec un environnement où le pare-feu Data Protector est activé.

Pour activer le pare-feu Data Protector dans la cellule entière, exécutez les commandes suivantes :

```
omnicc -firewall –all –enable_dp
```

Pour activer le pare-feu Data Protector dans une partie de la cellule, spécifiez les hôtes individuels au lieu de -all.

Par exemple, pour tester si la communication de l'agent de disque à l'agent de support est possible à travers le pare-feu, fermez le pare-feu en exécutant la commande suivante :

```
omnicc -firewall –host MAhost DAhost –enable_dp
```

En même temps que l'option -enable_dp, utilisez l'option -enable_os pour désactiver les règles Data Protector dans le pare-feu Windows.

Après avoir testé ces options, l'utilisateur peut fermer les pare-feu tiers (les routeurs, par exemple).

Utilisation des ports dans HPE Data Protector 9.09 et versions ultérieures

Le tableau qui suit fournit des informations sur les conditions préalables à remplir pour les différents composants Data Protector 9.09 ou versions ultérieures :

Hôtes Data Protector	Conditions préalables concernant les	Conditions préalables pour Data Protector	Conditions préalables de tiers pour

	ports	concernant les hôtes d'application	l'application
En tant que cible d'installation	Linux/Unix : • REXEC[1] (non sécurisé) : 512 • RSH (non sécurisé) : 514 • SSH : 22 Windows : Service SMB 445	Aucune	Aucune
En tant que Gestionnaire de cellule	• Inet : 5555/5565 • Hpdp-as : 7116 • Service IDB : 7112	Aucune	Aucune
En tant qu'Agent de disque HPE Data Protector	Inet : 5555/5565	Aucune	Aucune
En tant qu'Agent(s) d'intégration HPE Data Protector[4]	Inet : 5555/5565	Aucune	Aucune
En tant qu'Agent de support NDMP ou agent de support général HPE Data Protector	Inet : 5555/5565	Aucune	Système de déduplication Store Once[2] • Port de commande : 9387 • Port de données : 9388 NDMP Serveur [2] • Serveur : 10000 DDBoost[3] • NFS : 2049 • Réplication de fichier géré : 2051 • Mappeur de port NFS : 111

[1] Un seul port n'est nécessaire parmi REXEC/RSH/SSHD, selon la méthode d'installation.

[2] Pour des informations précises sur les autres ports pouvant être ouverts par des applications tierces, veuillez consulter la documentation des applications tierces.

[3] Pour plus d'informations sur les ports DDBoost, veuillez consulter le Guide de l'administrateur EMC® Data Domain® Boost pour OpenStorage.

[4] Sur un serveur Windows Hyper-V, les ports suivants doivent être ouverts pour la sauvegarde et la restauration Hyper-V

- **Instance WMI : 135 (Initialisation)**
- **Gestion à distance Windows (HTTPS) : 5986**

[5] Sur un serveur Windows Hyper-V, les ports suivants doivent être ouverts pour la sauvegarde et la restauration Hyper-V

Lors de l'établissement des règles de configuration de pare-feu, le processus de la première colonne doit être capable d'accepter de nouvelles connexions TCP (bit SYN défini) sur les ports définis dans la deuxième colonne à partir du processus figurant dans la troisième colonne.

De plus, le processus figurant dans la première colonne doit être capable de répondre à celui de la troisième colonne sur la connexion TCP (bit SYN non défini).

Par exemple, le processus Inet du système Agent de support doit pouvoir accepter de nouvelles connexions TCP du Gestionnaire de cellule sur le port 5555/5565. Un Agent de support doit être à même de répondre au Gestionnaire de cellule à l'aide de la connexion TCP existante. Il n'est pas obligatoire qu'un Agent de support soit capable d'ouvrir une connexion TCP.

Limites

- Cette fonctionnalité n'est pas disponible sur les hôtes OpenVMS et SCO. Si un agent de support (ou tout composant HPE Data Protector susceptible d'ouvrir des ports) est en cours d'exécution sur ces systèmes, l'utilisateur est toujours obligé d'ouvrir ces ports dans le pare-feu.

Agents de disque, de support et d'application dans la zone DMZ

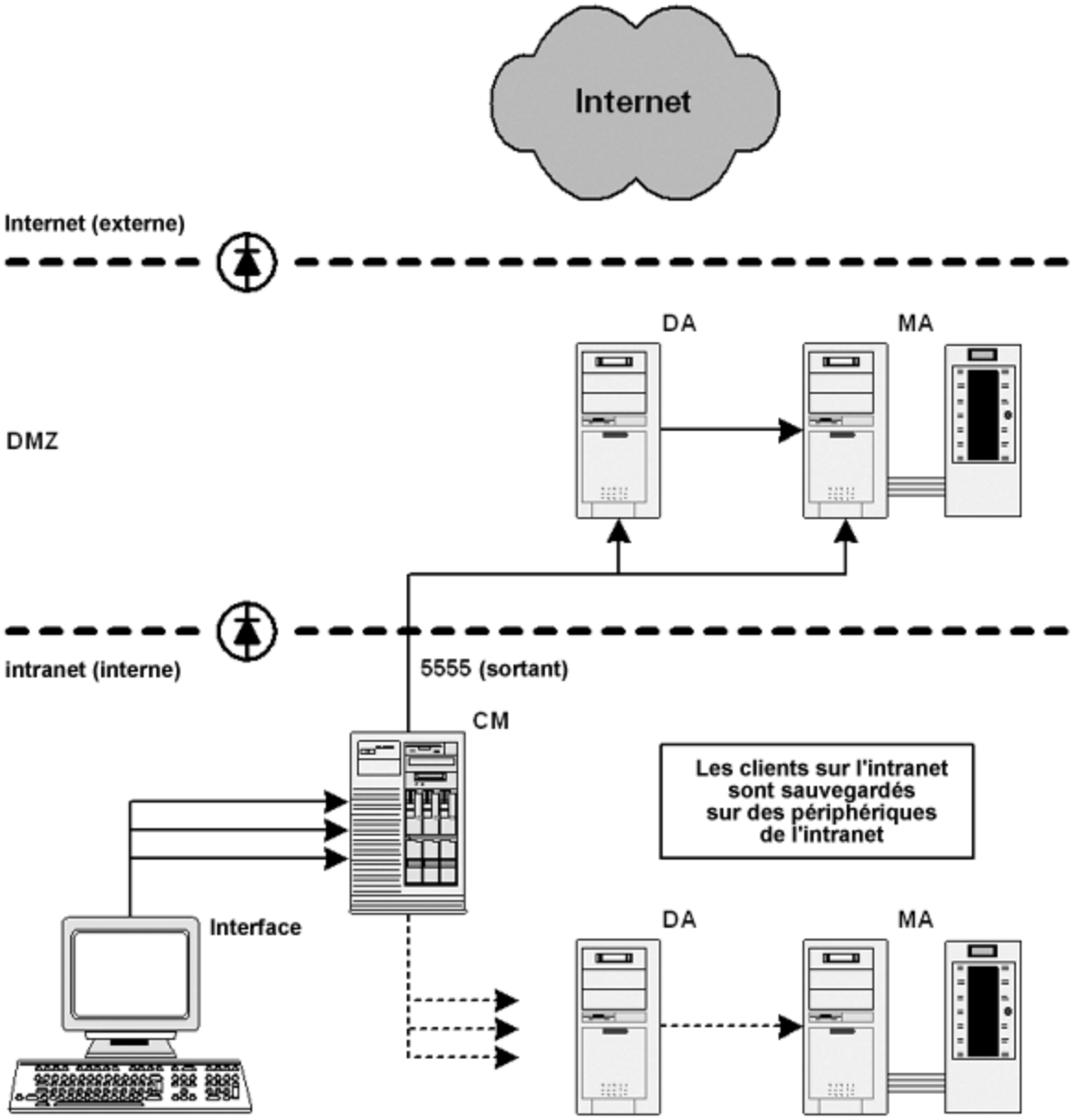
Vous pouvez configurer votre environnement de sauvegarde de sorte que le Gestionnaire de cellule et l'interface utilisateur soient sur l'intranet et certains Agents de disque, d'application et de support dans la zone DMZ.

Schémas de configuration

Ports ouverts

Limites

Schéma de configuration



Ports ouverts

HPE Data Protector ouvre les ports suivants pour la configuration :

1. L'Agent de disque et un Agent de support doivent pouvoir accepter des connexions du Gestionnaire de session sur le port 5555/5565.

- Autoriser les connexions du système CM sur le port 5555/5565 du système DA
- Autoriser les connexions du système CM sur le port 5555/5565 du système MA

2. Lorsque **reconnecter les connexions rompues** est activé, les systèmes MA et DA se connectent au Gestionnaire de session :
   - Autoriser les connexions des systèmes MA et DA sur le port 5555/5565 du système CM
3. L'agent d'application doit se connecter au Gestionnaire de session et au CRS :
   - Autoriser les connexions du système du serveur d'application sur le port 5555/5565 du système CM

> **REMARQUE :**
> Les points 2 et 3 autorisent des connexions de la DMZ à l'intranet, ce qui représente un risque potentiel pour la sécurité.

Limites

- Cette cellule peut sauvegarder les clients dans la DMZ ainsi que sur l'intranet. Cependant, chaque groupe de clients doit être sauvegardé sur des périphériques configurés sur des clients qui se trouvent du même côté du pare-feu.

  Si votre pare-feu ne limite pas les connexions entre l'intranet et la DMZ, il est possible de sauvegarder des clients de l'intranet sur des périphériques configurés sur des clients se trouvant dans la DMZ. Cependant, cela n'est pas recommandé, étant donné que les données sauvegardées de cette façon deviennent plus vulnérables.
- Si un périphérique de la DMZ est doté d'un mécanisme configuré sur un client séparé, ce dernier doit se trouver également dans la DMZ.

Chapitre 3: Utilisateurs et groupes d'utilisateurs

À propos de la gestion des utilisateurs

La fonctionnalité de gestion des utilisateurs de Data Protector fournit une couche de sécurité empêchant l'accès aux données et systèmes par des personnes non autorisées.

La sécurité repose sur les droits d'accès définis pour chaque utilisateur. Les personnes qui souhaitent utiliser Data Protector doivent être configurées en tant qu'utilisateurs de Data Protector. Les groupes d'utilisateurs et la grande variété de droits utilisateur disponibles vous permettent d'adapter en souplesse la configuration utilisateur de Data Protector à vos besoins en matière de sécurité.

Par défaut, les données sauvegardées sont masquées pour tous les utilisateurs, à l'exception du propriétaire de la sauvegarde. Les autres utilisateurs n'ont même pas la possibilité de déterminer si ces données ont été sauvegardées. Le cas échéant, vous pouvez les autoriser à voir les données à l'aide des droits utilisateur appropriés.

Utilisateurs

Pour utiliser Data Protector, vous devez être un utilisateur autorisé de Data Protector. Pour cela, vous devez posséder un compte Data Protector, interdisant tout accès non autorisé à Data Protector et aux données sauvegardées. Dans les petits environnements, une seule personne suffit pour effectuer les tâches de sauvegarde. Pour créer ce compte, les administrateurs Data Protector spécifient un nom de connexion utilisateur, les systèmes à partir desquels l'utilisateur peut se connecter et affectent l'utilisateur à un groupe d'utilisateurs Data Protector. Ces spécifications sont vérifiées chaque fois que l'utilisateur démarre l'interface utilisateur de Data Protector ou effectue certaines tâches.

Chaque utilisateur ne peut appartenir qu'à un seul groupe d'utilisateurs, Cela définit les droits utilisateur de cet utilisateur.

Vous pouvez configurer des utilisateurs UNIX et Windows :

UNIX

Les utilisateurs sont définis par leur nom de connexion, leur groupe d'utilisateurs UNIX et le système à partir duquel ils se connectent. Il est possible d'utiliser un caractère générique.

Windows

Les utilisateurs sont définis par leur nom de connexion, le domaine ou le groupe de travail Windows et le système à partir duquel ils se connectent. Il est possible d'utiliser un caractère générique.

Utilisateurs prédéfinis

Après l'installation initiale, tous les groupes d'utilisateur par défaut sont vides, sauf le groupe `admin`. Data Protector ajoute les utilisateurs suivants au groupe `admin` :

Gestionnaire de cellule	Compte utilisateur	Remarques
Gestionnaire de cellule sous UNIX	L'utilisateur `root` sur le Responsable de Cellule (`root`, *`any group`*, *`Cell Manager host`*).	Ce compte utilisateur ne doit pas être modifié. Il est nécessaire à un bon fonctionnement du démon CRS et d'autres processus sur le Gestionnaire de cellule. Seul cet utilisateur est initialement autorisé à gérer la cellule. Pour gérer la cellule à partir de tout autre client, ajoutez un nouvel utilisateur.
Gestionnaire de cellule Windows	Compte de service CRS, tel que spécifié pendant l'installation de Data Protector (limité à l'hôte du Gestionnaire de cellule).	Le compte de service CRS doit rester inchangé sauf en cas de modification des paramètres de connexion du service. Il est nécessaire à un bon fonctionnement du démon CRS et d'autres processus sur le Gestionnaire de cellule.
	Utilisateur qui a installé le Gestionnaire de cellule (administrateur de cellule initial).	Cet utilisateur est configuré en tant qu'administrateur de cellule initial et peut gérer la cellule à partir de tous les clients. Il est recommandé de modifier ce compte utilisateur une fois l'installation de Data Protector terminée. Spécifiez le client à partir duquel vous allez gérer la cellule au lieu d'autoriser l'accès depuis n'importe quel hôte. Si vous allez utiliser un autre compte, ajoutez-le, puis supprimez l'administrateur de cellule initial ou autorisez-le sur le Gestionnaire de cellule.
	Le compte du système local sur le Responsable de Cellule (`SYSTEM`, `NT AUTHORITY`, *`Cell Manager host`*).	Ce compte est fourni en cas de configuration du service CRS pour une connexion en tant que compte système local.

Nous vous conseillons de définir des groupes spécifiques pour chaque type d'utilisateur dans un environnement afin de réduire au strict minimum les droits qui leur sont attribués.

Pour de plus amples informations sur l'utilisateur `java`, consultez le *Guide d'installation HPE Data Protector*.

> **IMPORTANT :**
> `Admin` Les capacités du groupe sont très puissantes. Un membre du groupe utilisateur Data Protector `admin` a des capacités de l'administrateur du système pour toute la cellule. Pour de plus amples informations sur la sécurité, consultez le *Guide d'installation HPE Data Protector*.

Groupes d'utilisateurs

Un groupe d'utilisateurs rassemble des utilisateurs disposant des mêmes droits. L'administrateur simplifie la configuration utilisateur en regroupant les utilisateurs d'après leurs besoins en matière d'accès. Il réunit dans un même groupe les utilisateurs qui nécessitent les mêmes droits. Certains utilisateurs peuvent, par exemple, devoir disposer de droits permettant de surveiller les sessions dans la cellule, de configurer la sauvegarde ou de restaurer des fichiers.

Data Protector propose des groupes d'utilisateurs par défaut. Vous pouvez les utiliser tels quels, les modifier ou en créer de nouveaux.

Groupes utilisateurs prédéfinis

Pour simplifier la configuration, Data Protector propose trois groupes d'utilisateurs prédéfinis, dotés des droits suivants :

Droit utilisateur	Admin	Opérateur	L'utilisateur
Configuration des clients	✓		
Configuration utilisateur	✓		
Configuration des périphériques	✓		
Configuration support	✓	✓	
Rapports et notifications	✓		
Démarrer la sauvegarde	✓	✓	
Démarrer la spécification de sauvegarde	✓	✓	
Enregistrer spécification de sauvegarde	✓		
Sauvegarder en tant que root	✓		
Permuter propriété de session	✓	✓	
Contrôle	✓	✓	
Abandonner	✓	✓	

Demande de montage	✓	✓	
Démarrer la restauration	✓	✓	✓
Restaurer vers autre client	✓		
Restaurer à partir d'autres utilisateurs	✓	✓	
Restaurer en tant que root	✓		
Voir objets privés	✓	✓	

Après l'installation initiale, tous les groupes prédéfinis sont vides, hormis le groupe d'utilisateurs `admin`.

> **IMPORTANT :**
> Les fonctions d'administrateur confèrent un pouvoir très important à l'utilisateur ! Les membres du groupe d'utilisateurs admin de Data Protector `admin` disposent des droits administrateur système sur toute la cellule.

Les droits utilisateur définis dans le Gestionnaire de cellule déterminent la disponibilité de l'interface de Gestionnaire de cellule Data Protector ou des contextes d'interface sur l'ordinateur sur lequel vous vous connectez au Gestionnaire de cellule. Par exemple, si vous ne disposez que du droit utilisateur Démarrer restauration, seul le contexte de restauration est disponible lorsque vous installez le composant Interface utilisateur.

Droits utilisateur disponibles

Data Protector propose une grande variété de droits utilisateur permettant de mettre en œuvre des fonctionnalités de sécurité avancées. Pour des informations plus détaillées sur les droits d'utilisateur, consultez Aide de HPE Data Protector.

Fourniture d'accès aux services Web pour les utilisateurs

HPE Data Protectorutilise les services internet pour la communication et l'administration interne. Certains modules HPE Data Protector, tels que les GUI sont configurés par défaut pour accéder à ces services internet. Cependant, pour certains modules, tels que le plug-in Advanced GRE Web et les API REST, vous devez explicitement fournir l'accès internet à l'utilisateur.

Vous pouvez fournir l'accès au service internet soit en utilisant le GUI HPE Data Protectorou en utilisant le CLI.

> **REMARQUE :**
> WebAccess ne peut pas être activé pour les membres de la classe Data Protector**utilisateur**.

Utilisation du GUI HPE Data Protector

Exécutez les étapes qui suivent :

1. Dans la liste de contexte, cliquez sur **Utilisateurs.**
2. Dans le volet exploration, élargissez les **Utilisateurs** et sélectionnez l'utilisateur auquel vous souhaitez fournir l'accès au service internet.
3. Dans l'onglet Général des Propriétés de la boîte de dialogue Utilisateur HPE Data Protector, cochez la case **Accès Internet**. La fenêtre d'authentification s'ouvre.
4. Saisir le mot de passe dans la fenêtre de texte mot de passe, puis cliquez sur **OK**.
5. Cliquez sur **Appliquer**.

Utilisation de la ligne de commande

Exécutez une des commandes suivantes selon si vous souhaitez créer de nouvelles propriétés utilisateur ou mise à jour d'un utilisateur existant :

- Créez un nouvel utilisateur avec l'accès au service internet :
  `omniusers -add -type {U | W} -name <UserName> -webaccess enable -passwd <Password>`
- Mettre à jour l'utilisateur existant :
  `omniusers -webaccess enable -name UserName -passwd Password -group GroupOrDomainName -client ClientName`

Pour de plus amples informations sur la commande `omniusers`, consultez le guide *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Configuration de clients

Ajout d'un utilisateur

Pour configurer un utilisateur pour Data Protector, vous devez l'ajouter à un groupe d'utilisateurs existant.

Conditions préalables

Vous devez disposer du droit Configuration utilisateur pour être en mesure d'ajouter des utilisateurs.

Procédure

1. Dans la liste de contexte, cliquez sur **Utilisateurs.**
2. Dans la fenêtre de navigation, développez l'élément **Utilisateurs**.
3. Cliquez avec le bouton droit sur le groupe auquel vous souhaitez ajouter un utilisateur.
4. Cliquez sur **Ajouter/Supprimer utilisateurs** pour lancer l'assistant.
5. Dans la boîte de dialogue Ajouter/Supprimer utilisateurs, saisissez les propriétés spécifiques de l'utilisateur. Lorsque vous saisissez le **Nom** et le **Groupe/Domaine** ou le **Groupe UNIX**, assurez-vous qu'il s'agit bien des informations relatives à un utilisateur existant sur votre réseau.
6. Cliquez sur **>>** pour ajouter l'utilisateur à la liste.

> **CONSEIL :**
> Vous pouvez également supprimer un utilisateur, en le sélectionnant dans la liste des utilisateurs, puis en cliquant sur **<<**.

7. Cliquez sur **Terminer** pour quitter l'assistant.

L'utilisateur est ajouté au groupe et dispose des droits utilisateur associés à ce groupe.

Affichage d'un utilisateur

Pour afficher les propriétés spécifiques d'un utilisateur, procédez comme suit.

Conditions préalables

Vous devez être un utilisateur Data Protector.

Procédure

1. Dans la liste de contexte, cliquez sur **Utilisateurs.**
2. Dans la fenêtre de navigation, développez l'élément **Utilisateurs**.
3. Cliquez sur le nom du groupe d'utilisateurs dont fait partie l'utilisateur.
4. Dans la zone de résultats, double-cliquez sur l'utilisateur que vous souhaitez afficher.

Les propriétés spécifiques de l'utilisateur s'affichent dans la zone de résultats.

Modification des propriétés d'un utilisateur

Vous pouvez modifier les propriétés indiquées lors de la configuration d'un utilisateur pour Data Protector. En affectant l'utilisateur à un autre groupe, vous modifiez ses droits utilisateur.

Conditions préalables

Vous devez disposer du droit Configuration utilisateur pour pouvoir modifier les propriétés de l'utilisateur.

Procédure

1. Dans la liste de contexte, cliquez sur **Utilisateurs.**
2. Dans la fenêtre de navigation, développez l'élément **Utilisateurs**.
3. Cliquez sur le nom du groupe d'utilisateurs dont fait partie l'utilisateur.
4. Dans la zone de résultats, cliquez avec le bouton droit sur l'utilisateur que vous souhaitez modifier.
5. Cliquez sur **Propriétés**.
6. Saisissez les propriétés que vous souhaitez modifier. Lorsque vous modifiez le **Nom** et le **Groupe/domaine** ou le **groupe UNIX**, assurez-vous qu'il s'agit bien des informations concernant

un utilisateur existant sur votre réseau.

7. Cliquez sur **Appliquer**.

Déplacement d'un utilisateur vers un autre groupe

Pour modifier les droits d'un utilisateur, il convient de le déplacer vers un autre groupe.

Conditions préalables

Vous devez disposer du droit Configuration utilisateur pour être en mesure de déplacer des utilisateurs.

Procédure

1. Dans la liste de contexte, cliquez sur **Utilisateurs.**
2. Dans la fenêtre de navigation, développez l'élément **Utilisateurs**.
3. Cliquez sur le nom du groupe d'utilisateurs dont fait partie l'utilisateur.
4. Dans la zone de résultats, cliquez avec le bouton droit de la souris sur l'utilisateur que vous souhaitez déplacer.
5. Cliquez sur **Déplacer**.
6. Dans la liste Groupe cible, choisissez le groupe d'utilisateurs approprié, puis cliquez sur **OK**.

L'utilisateur est supprimé du groupe d'origine et ajouté au groupe sélectionné. Il bénéficie désormais des droits de ce nouveau groupe d'utilisateurs.

Suppression d'un utilisateur

Pour supprimer un utilisateur, il convient de le retirer du groupe d'utilisateurs dans lequel il est configuré.

Conditions préalables

Vous devez disposer du droit Configuration utilisateur pour être en mesure de supprimer des utilisateurs.

Procédure

1. Dans la liste de contexte, cliquez sur **Utilisateurs.**
2. Dans la fenêtre de navigation, développez l'élément **Utilisateurs**.
3. Cliquez sur le nom du groupe d'utilisateurs dont fait partie l'utilisateur.
4. Dans la zone de résultats, cliquez avec le bouton droit de la souris sur l'utilisateur que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
5. Confirmez l'opération.

L'utilisateur est supprimé du groupe et ne peut plus utiliser Data Protector.

CONSEIL :
Vous pouvez également supprimer des utilisateurs dans la boîte de dialogue Ajouter/Supprimer utilisateurs.

Configuration des groupes d'utilisateurs

Ajout d'un groupe d'utilisateurs

Les groupes d'utilisateurs Data Protector définis par défaut sont généralement suffisants. Vous pouvez cependant définir vos propres groupes d'utilisateurs pour contrôler l'attribution des droits dans votre environnement Data Protector en fonction de vos besoins. Toutefois, avant de créer un groupe, vérifiez s'il ne suffit pas de modifier simplement un groupe existant.

Conditions préalables

Vous devez disposer des droits **Configuration utilisateur**.

Procédure

1. Dans la liste de contexte, cliquez sur **Utilisateurs.**
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur **Utilisateurs**.
3. Cliquez sur **Ajouter groupe d'utilisateurs** ou Sessions pour ouvrir l'assistant.
4. Saisissez le nom et la description du nouveau groupe.
5. Cliquez sur **Next**.
6. Définissez les droits utilisateur spécifiques au nouveau groupe.
7. Cliquez sur **Terminer** pour quitter l'assistant

Le nouveau groupe d'utilisateurs vide est ajouté à Data Protector.

Affichage d'un groupe d'utilisateurs

Pour afficher les propriétés spécifiques d'un groupe d'utilisateurs, procédez comme suit.

Conditions préalables

Vous devez être un utilisateur Data Protector.

Procédure

1. Dans la liste de contexte, cliquez sur **Utilisateurs.**
2. Dans la fenêtre de navigation, développez l'élément **Utilisateurs**.
3. Cliquez avec le bouton droit sur le groupe d'utilisateurs.
4. Cliquez sur **Propriétés**.

Les propriétés du groupe d'utilisateurs s'affichent dans la zone de résultats.

Modification des droits utilisateur

Vous pouvez modifier les droits attribués à un groupe d'utilisateurs (à l'exception du groupe d'utilisateurs `admin`) afin que celui-ci réponde mieux à vos besoins. Vous devez attribuer au moins un droit à chaque groupe d'utilisateurs. Vous pouvez également modifier les propriétés de chaque utilisateur d'un groupe, par exemple, le domaine ou le groupe d'utilisateurs auquel il appartient, ou encore son vrai nom. Si vous sélectionnez un groupe qui ne contient aucun utilisateur, la zone de résultats affiche les propriétés du groupe. Si vous sélectionnez un groupe qui contient des utilisateurs, la zone de résultats affiche la liste des utilisteurs du groupe. Vous pouvez également modifier les propriétés de chaque utilisateur d'un groupe en cliquant sur l'utilisateur concerné.

Conditions préalables

- Il ne doit pas s'agir du groupe d'utilisateurs `admin`.
- Vous devez être titulaire des droits `User configuration`.

Procédure

1. Dans la liste de contexte, cliquez sur **Utilisateurs.**
2. Dans la fenêtre de navigation, développez l'élément **Utilisateurs**.
3. Cliquez avec le bouton droit sur le groupe d'utilisateurs à modifier.
4. Cliquez sur **Propriétés**, puis sur l'onglet **Droits utilisateur**.
5. Modifiez les droits en fonction de vos besoins. Pour attribuer tous les droits utilisateur au groupe, cliquez sur **Sélectionner tout**. Si vous souhaitez modifier un grand nombre de droits utilisateur, cliquez sur **Désélectionner tout** pour supprimer tous les droits du groupe d'utilisateurs, puis lui en attribuer au moins un.
6. Cliquez sur **Appliquer**.

Les droits utilisateur spécifiés sont attribués au groupe, ainsi qu'à tous les membres de ce groupe.

Suppression d'un groupe d'utilisateurs

Vous pouvez supprimer les groupes d'utilisateurs dont vous n'avez plus besoin (à l'exception du groupe `admin`).

Conditions préalables

- Il ne doit pas s'agir du groupe d'utilisateurs `admin`.
- Vous devez être titulaire des droits `User configuration`.

Procédure

1. Dans la liste de contexte, cliquez sur **Utilisateurs.**
2. Dans la fenêtre de navigation, développez l'élément **Utilisateurs**.
3. Cliquez avec le bouton droit sur le groupe d'utilisateurs à supprimer.
4. Cliquez sur **Supprimer**.

Le groupe d'utilisateurs et tous ses membres sont supprimés de Data Protector.

Chapitre 4: Base de données interne

A propos de la base de données IDB

La base de données interne (IDB) est une base de données intégrée à Data Protector, située sur le Gestionnaire de cellule, qui stocke des informations sur les données sauvegardées, le support sur lequel elles résident, le résultat des sessions de sauvegarde, de restauration, de copie, de consolidation et de vérification d'objet, ainsi que de gestion des supports et les périphériques et bibliothèques qui sont configurés.

Quel est le rôle de l'IDB ?

Les informations stockées dans l'IDB permettent d'effectuer les opérations suivantes :

- Restauration rapide et facile

  Vous pouvez parcourir les fichiers et répertoires à restaurer. Vous pouvez retrouver rapidement les supports requis pour une restauration et donc accélérer considérablement le processus.
- Gestion de la sauvegarde

  vous pouvez vérifier les résultats des sessions de sauvegarde.
- Gestion des supports

  Vous pouvez allouer des supports pendant des sessions de sauvegarde, de copie d'objets et de consolidation d'objet, effectuer un suivi des opérations de gestion et des attributs des supports, regrouper des supports dans différents pools de supports et effectuer le suivi des emplacements des supports dans les bibliothèques de bandes.
- Gestion de cryptage/décryptage : Les informations stockées dans la base de données IDB permettent à Data Protector d'allouer des clés de cryptage aux sessions de sauvegarde ou de copie, et de fournir la clé de décryptage requise pour la restauration des objets sauvegarde cryptés.

À propos de la taille et de la croissance de l'IDB

La taille de l'IDB peut augmenter énormément et avoir un effet important sur les performances des sauvegardes et sur le Gestionnaire de cellule. L'administrateur Data Protector doit comprendre l'IDB et décider de la nature et de la durée de validité des informations qu'elle contient. C'est à l'administrateur qu'il incombe d'équilibrer les durées et fonctionnalités de restauration avec la taille et la croissance de l'IDB. Data Protector propose deux paramètres principaux pour vous aider à équilibrer vos besoins : le niveau de journalisation et la protection du catalogue.

Sauvegardes régulières de l'IDB

HPE recommande fortement de sauvegarder l'IDB régulièrement. Pour plus d'informations, voir Configuration de la sauvegarde de l'IDB.

Architecture de la base de données IDB

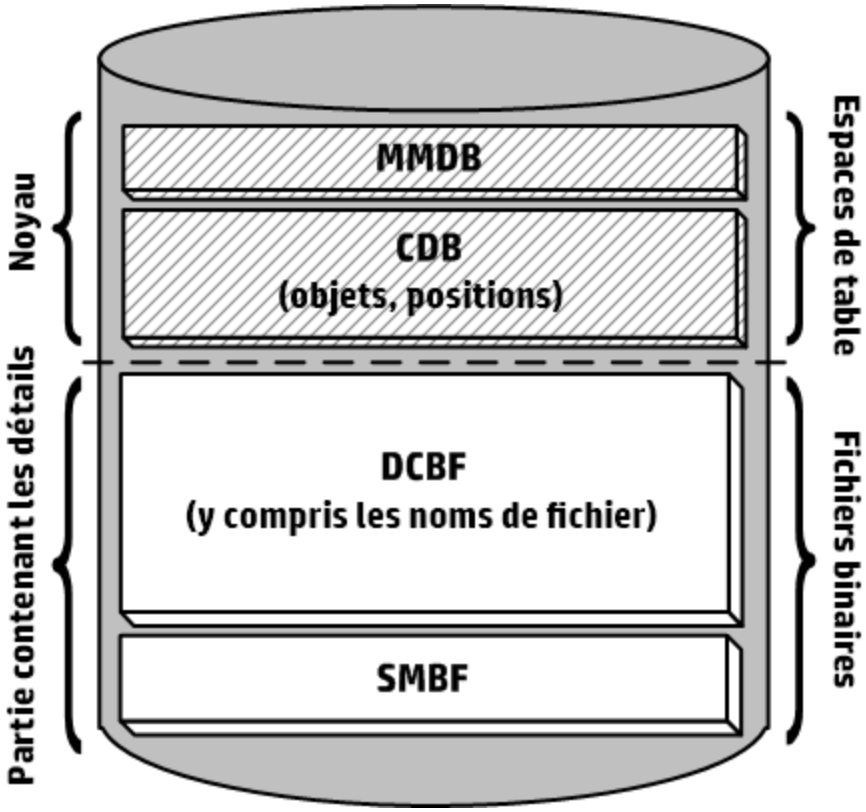
La base de données interne (IDB) se compose des éléments suivants :

- Base de données de gestion des supports (MMDB)
- Base de données catalogue (CDB)
- Fichiers binaires de catalogue des détails (DCBF)
- Fichiers binaires de messages de session (SMBF)
- Porte-clés de cryptage et fichiers de catalogue

Chacune des parties de l'IDB stocke certaines informations spécifiques à Data Protector (enregistrements), joue sur la taille de l'IDB et sur sa croissance de différentes manières, et est stockée dans un répertoire distinct du Gestionnaire de cellule.

parties d'IDB

Architecture de la base de données



Les parties MMDB et CDB sont implémentées avec une base de données intégrée composée d'espaces de table. Cette base de données est contrôlée par les processus `hpdp-idb`, `hpdp-idb-cp` et `hpdp-as`. Les parties CDB (objets et positions) et MMDB constituent la partie centrale de l'IDB.

Les parties DCBF et SMBF de l'IDB se composent de fichiers binaires. Les mises à jour sont directes (pas de transactions).

Dans l'environnement Manager-of-Managers (MoM), la partie MMDB peut être déplacée vers un système central pour créer la base de données de gestion centrale des supports (CMMDB).

Base de données de gestion des supports (MMDB)

Enregistrements MMDB

La Base de données de gestion des supports stocke des informations à propos des éléments suivants :

- Périphériques configurés, bibliothèques, lecteurs de bibliothèque et emplacements
- Data Protector support
- Pools de supports configurés et magazines de supports

Taille et croissance de la MMDB

La MMDB ne grandit pas beaucoup en taille. La majeure partie de la MMDB est généralement occupée par des informations sur les supports Data Protector.

Emplacement de la MMDB

La MMDB se trouve dans le répertoire suivant :

Systèmes Windows : *données_programme_Data_Protector*\server\db80\idb

Systèmes UNIX : /var/opt/omni/server/db80/idb

Base de données catalogue (CDB)

Enregistrements CDB

La Base de données de catalogue stocke des informations à propos des éléments suivants :

- Sessions de sauvegarde, restauration, copie d'objet, consolidation d'objet, vérification d'objet et gestion des supports. Il s'agit de la copie des informations envoyées à la fenêtre du moniteur Data Protector.
- Les objets sauvegardés, leurs versions et les copies d'objets. En cas de versions d'objet cryptées, les identifiants de clé (KeyID-StoreID) sont également stockés.
- Les positions des objets sauvegardés sur les supports. Pour chaque objet sauvegardé, Data Protector stocke des informations sur les supports et segments de données utilisés pour la sauvegarde. La même chose est effectuée pour les copies d'objet et les miroirs d'objet.

Taille et croissance de la CDB (objets et positions)

Les enregistrements du CDB occupent une partie de l'espace mineure dans l'IDB.

Emplacement de la CDB

La CDB se trouve dans le répertoire suivant :

Systèmes Windows : *données_programme_Data_Protector*\server\db80\idb

Systèmes UNIX : /var/opt/omni/server/db80/idb

Fichiers binaires de catalogue des détails (DCBF)

Informations DCBF

La partie fichiers binaires du catalogue des détails stocke des informations sur ce qui suit :

- Noms de chemin des fichiers sauvegardés (noms de fichiers) ainsi que les noms des systèmes clients. Les noms de fichier des fichiers créés entre les sauvegardes sont ajoutés à la partie DCBF.
- Métadonnées des fichiers. Il s'agit des informations sur les versions des fichiers sauvegardés, leurs tailles de fichier, les dates de modification et les positions des copies de sauvegarde sur le support de sauvegarde.

Un fichier binaire DC (catalogue des détails) est créé par support Data Protector utilisé pour la sauvegarde. Lorsque le support est écrasé, son ancien fichier binaire est supprimé et un nouveau fichier est créé.

Taille et croissance de la partie DCBF

Dans un environnement où les sauvegardes du système de fichiers utilisent typiquement l'option Journaliser tout, la partie DCBF constitue la plus grande partie de l'IDB. Le niveau de journalisation et la protection du catalogue peuvent être utilisés pour spécifier ce qui est réellement stocké dans l'IDB et pour quelle durée.

Par défaut, cinq répertoires DC sont configurés pour les fichiers binaires DC. Si le nombre de supports de sauvegarde ou de fichiers binaires DC grandit beaucoup ou que vous avez des problèmes d'espace disque, vous pouvez en créer davantage pour agrandir la taille de votre IDB.

La partie la plus grande et la plus rapide du DCBF est la partie des noms de fichier.

La croissance de la part des noms de fichiers est proportionnelle à la croissance et à la dynamique de l'environnement de sauvegarde ainsi qu'au nombre de sauvegardes.

Un fichier ou un répertoire occupe approximativement 100 bits dans l'IDB.

Emplacement de la partie DCBF

Par défaut, le DCBF se situe dans les sous-répertoires dcbf0 par dcbf4 dans le répertoire suivant :

Systèmes Windows : *données_programme_Data_Protector*\server\db80\dcbf

Systèmes UNIX : /var/opt/omni/server/db80/dcbf

Considérez l'espace disque du Gestionnaire de cellule et déplacez le répertoire DC, si nécessaire. Vous pouvez créer d'autres répertoires DC et les déplacer sur différents disques.

Fichiers binaires de messages de session (SMBF)

Enregistrements SMBF

Les fichiers binaires de messages de session contiennent les messages générés lors des sessions de sauvegarde, de restauration, de copie d'objets, de consolidation d'objet, de vérification d'objet et de gestion des supports. Chaque session génère un fichier binaire. Les fichiers sont regroupés par année et par mois.

Taille et croissance de la partie SMBF

La taille de SMBF dépend des éléments suivants :

- Nombre de sessions effectuées.
- Nombre de messages dans une session. Un message de session occupe environ 200 octets. Vous pouvez modifier le volume des messages affichés lors des opérations de sauvegarde, restauration et gestion des supports en modifiant l'option Niveau de rapport. Cela joue sur le nombre de messages stockés dans l'IDB.

Emplacement de la partie SMBF

La partie SMBF se trouve dans le répertoire suivant :

Systèmes Windows : *données_programme_Data_Protector*\server\db80\msg

Systèmes UNIX : /var/opt/omni/server/db80/msg

Vous pouvez relocaliser le répertoire en éditant l'option globale SessionMessageDir.

Porte-clés de cryptage et fichiers de catalogue

Toutes les clés créées lors de sauvegardes cryptées, manuellement ou automatiquement, sont stockées dans une banque de clés. Les clés peuvent également être utilisées pour les sessions de copie d'objet, de vérification d'objet et de restauration. En cas de cryptage matériel, elles peuvent également être utilisées pour les sessions de consolidation d'objet.

Dans le cas du cryptage matériel, les identifiants de clé (chacun composé d'un KeyID et d'un StoreID) sont mappés sur les versions cryptées des objets. Ce mappage est stocké dans la base de données du catalogue. Différents objets sur un support peuvent avoir différentes clés de cryptage (logicielles).

Pour le cryptage matériel, les identifiants de clé sont mappés sur l'ID du support et ces mappages sont stockés dans un fichier de catalogue. Ce fichier contient les informations nécessaires pour permettre l'exportation d'un support crypté vers une autre cellule.

Emplacement de la banque de clés

La banque de clés se trouve dans le répertoire suivant :

Systèmes Windows : *données_programme_Data_Protector*\server\db80\keystore

Systèmes UNIX : `/var/opt/omni/server/db80/keystore`

Emplacement des fichiers de catalogue

Les fichiers du catalogue se trouvent dans le répertoire suivant :

Systèmes Windows : *`données_programme_Data_Protector`*`\server\db80\keystore\catalog`

Systèmes UNIX : `/var/opt/omni/server/db80/keystore/catalog`

Fonctionnement de la base de données IDB

Découvrez le comportement de l'IDB lors des opérations Data Protector suivantes :

- Sauvegarde
- Restaurer
- Copie d'objet et consolidation d'objet
- Vérification d'objet
- Exportation de supports
- Supprimer le Catalogue de détails

Sauvegarde

Lorsqu'une session de sauvegarde est commencée, un enregistrement de session est créé dans l'IDB. Aussi, pour chaque objet de la session, un enregistrement de la version de l'objet est créé. Les deux enregistrements sont stockés dans la partie CDB et ont plusieurs attributs. Le Gestionnaire de session de sauvegarde met à jour le support au cours d'une sauvegarde. Tous les enregistrements de support sont stockés dans la partie MMDB et sont affectés pour une sauvegarde en fonction des stratégies.

Lorsqu'un segment de données (et un segment de catalogue après lui) est écrit sur la bande, un enregistrement de position de support est stocké dans la CDB pour chaque version de l'objet qui faisait partie de ce segment de données. De plus, le catalogue est stocké dans le fichier binaire de catalogue des détails (DC). Un fichier binaire DC est conservé par support Data Protector. Le fichier binaire DC possède un nom au format suivant : *`MediumID_TimeStamp`*`.dat`. Le nom ne change pas lorsque des sauvegardes s'ajoutent au même support. Si un support est écrasé lors d'une sauvegarde, son ancien fichier binaire DC est supprimé et un nouveau fichier binaire DC est créé.

Tous les messages de session générés lors de sauvegardes sont stockés dans des fichiers binaires de messages de session (la partie SMBF).

Sauvegarde IDB et fichiers journaux archivés

En fonction de la configuration de votre spécification de base de données interne, le processus de sauvegarde de l'IDB peut supprimer les anciens fichiers journaux archivés, et commence à en créer de nouveaux nécessaires pour la récupération de l'IDB.

Restaurer

Lors de la configuration de la restauration, Data Protector effectue un ensemble de requêtes sur les parties DCB et DCBF pour permettre aux utilisateurs de parcourir les systèmes de fichiers virtuels des données sauvegardées. Ces requêtes de parcours sont effectuées en deux étapes. La première étape consiste à sélectionner un objet spécifique (système de fichiers ou lecteur logique). Si cet objet a de nombreuses versions de sauvegarde enregistrées, cela peut prendre du temps, car Data Protector analyse la partie DCBF pour construire un cache de recherche pour la navigation ultérieure. La deuxième étape est la navigation dans les répertoires.

Après avoir sélectionné des versions spécifiques de fichiers, Data Protector détermine les supports requis et localise les enregistrements de position de support utilisés par les fichiers sélectionnés. Ces supports sont lus par les Agents de support et les données sont envoyées aux Agents de disque qui restaurent les fichiers sélectionnés.

Copie d'objet et consolidation d'objet

Lors d'une session de copie ou de consolidation d'objet, les mêmes processus sont exécutés que pour les sessions de sauvegarde et de restauration. Les données sont essentiellement lues à partir du support source comme s'il était restauré et écrites sur le support cible comme s'il était sauvegardé. Une session de copie ou de consolidation d'objet a le même effet sur le fonctionnement de l'IDB que la sauvegarde et la restauration. Pour plus de détails, voir les sections précédentes.

Vérification d'objet

Au cours d'une session de vérification d'objet, les mêmes traitements de la base de données ont lieu comme au cours d'une session de restauration. Pour simplifier, les données sont lues depuis le support source, comme si elles étaient en train d'être restaurées, et sont envoyées aux Agents de disque hôtes, où la vérification est effectuée. Une session de vérification d'objet a le même effet sur le fonctionnement d'IDB qu'une session de restauration. Pour plus de détails, voir la section Restauration ci-dessus.

Tous les messages de session générés lors des sessions de vérification sont stockés dans des fichiers binaires de messages de session.

Exportation de supports

Lorsqu'un support est exporté, les éléments suivants sont supprimés :

- Tous les enregistrements de position de support de ce support sont supprimés de la partie CDB.
- Tous les objets qui n'ont plus de position sur des autres supports sont supprimés de la partie CDB.
- Les sessions obsolètes (dont les supports ont été écrasés ou exportés) sont supprimées. Les messages de sessions de telles sessions sont également supprimés.
- L'enregistrement de support est supprimé de la partie MMDB et le fichier binaire DC pour ce support est supprimé de la partie DCBF.

Supprimer le Catalogue de détails

Lorsque le catalogue des détails est supprimé pour un support spécifique, son fichier binaire DC est supprimé. Le même résultat est obtenu en supprimant la protection du catalogue pour toutes les versions sur ce support (la prochaine maintenance quotidienne des fichiers binaires DC supprime le fichier binaire). Tous les enregistrements restent sur les parties DCB et MMDB et il est possible d'exécuter une restauration depuis de tels supports (cependant, la navigation n'est pas possible).

Configuration de la base de données interne

Configuration de la base de données IDB

La configuration de la base de données interne vous aide à gérer ce qui suit :

- La taille de l'IDB et l'espace disque disponible
- L'emplacement des répertoires de l'IDB
- La sauvegarde de l'IDB elle-même, nécessaire en cas d'endommagement de l'IDB ou de sinistre
- Configuration des rapports et notifications de l'IDB

Vous devez effectuer des préparations avancées pour pouvoir récupérer l'IDB à n'importe quel moment dans le temps. La récupération de l'IDB restaure les informations stockées dans l'IDB et s'avère capitale pour restaurer des données sauvegardées en cas de sinistre survenant sur le Gestionnaire de cellule. La préparation pour la récupération de l'IDB consiste à :

- Vérifier les considérations de robustesse
- Déplacer les répertoires de l'IDB
- Configurer la sauvegarde de l'IDB
- Sauvegarder l'IDB régulièrement

Une fois l'IDB configurée, sa maintenance est réduite au minimum et consiste principalement à intervenir sur les notifications et les rapports.

Allocation d'espace disque pour la base de données IDB

L'espace disque occupé par la base de données interne sur le Gestionnaire de cellule peut considérablement augmenter avec le temps. Vous devez prévoir l'allocation de l'espace disque nécessaire en tenant compte de l'évolution de vos besoins.

Conditions préalables

- Vous devez bien comprendre comment les facteurs clés déterminent la croissance de l'IDB (nombre de fichiers, variations de fichiers, croissance de l'environnement, etc.).
- Vous devez définir le niveau de journalisation et les stratégies de protection de catalogue en fonction des besoins de votre environnement et de l'espace disque disponible.

- Vous devez également estimer la taille future de l'IDB (espace disque nécessaire pour ses besoins ultérieurs).

Quel est l'espace disque nécessaire ?

L'espace disque nécessaire pour l'IDB varie considérablement selon les différents aspects et stratégies de configuration utilisés lors de la définition et de l'exécution des sauvegardes.

Vous trouverez ci-après un scénario simplifié d'un environnement exigeant environ 900 Mo d'espace disque pour l'IDB après trois mois, avec une croissance réduite par la suite :

- 100 systèmes à sauvegarder (10 000 fichiers chacun, aucun serveur de messagerie)
- 350 Go de données au total.
- Des sauvegardes de système de fichiers avec environ 3 % de nouveaux fichiers par mois.
- Une sauvegarde complète et quatre sauvegardes incrémentales par semaine
- Le niveau de journalisation est Journaliser tout (pour pouvoir explorer facilement les noms de fichiers avant la restauration). Il s'agit de l'option de journalisation la plus exigeante.
- La protection de catalogue définie est de trois mois pour les sauvegardes complètes et de deux semaines pour les sauvegardes incrémentales.

> **REMARQUE :**
> Les configurations importantes ou les longues périodes de protection de catalogue requièrent plus de 20 Go pour l'IDB.

Que faut-il prévoir ?

En général, la taille de l'IDB augmente rapidement au début (jusqu'à ce que les périodes de rétention du catalogue soient atteintes). Ensuite, la croissance de l'IDB dépend principalement des variations des systèmes qui possèdent un fort taux de nouveaux fichiers par mois et de la croissance de l'environnement (nouveaux systèmes à sauvegarder).

Il est important de comprendre comment la taille de l'IDB augmente :

- La taille de la partie des noms de fichier de l'IDB croît en fonction du nombre de sauvegardes, du nombre de fichiers dans la cellule et de la durée de protection de catalogue.
- Prévoir l'espace de stockage occupé par les fichiers journaux archivés n'est pas simple. Les principaux facteurs déterminant la taille sont le nombre de nouveaux noms de fichier sauvegardés et le volume global des activités de sauvegarde (ou les semaines, si les sauvegardes planifiées représentent l'opération principale) entre les sauvegardes de l'IDB.

Emplacement des répertoires de la base de données IDB

La base de données interne est stockée dans le Gestionnaire de cellule. Vous voudrez peut-être déplacer certains répertoires de l'IDB et répondre aux recommandations pour optimiser la robustesse.

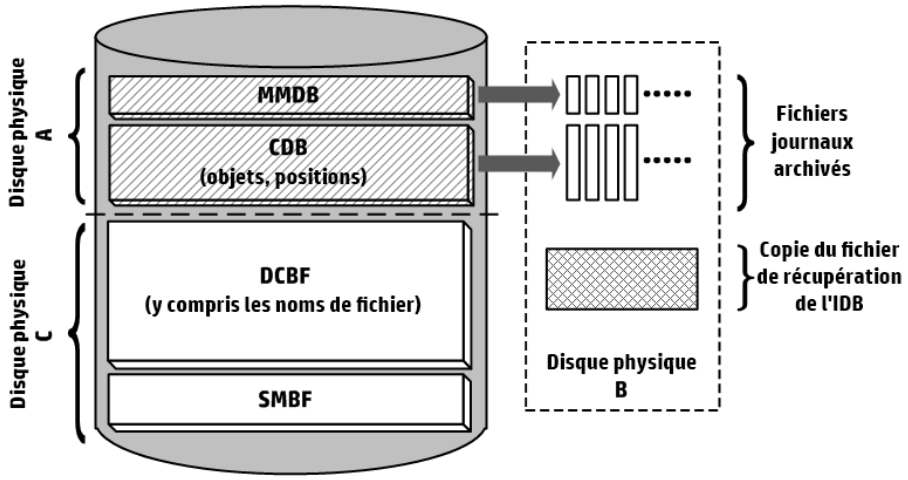
Limites

- Les fichiers de l'IDB peuvent être situés uniquement sur les volumes se trouvant sur des disques connectés localement (non montés avec NFS ou mappés en tant que dossiers réseau partagés).
- Si l'IDB est installée dans un cluster, elle doit être installée sur des volumes du groupe de clusters (Microsoft Cluster Server) ou paquet de clusters (HPE Serviceguard).
- Si l'IDB est installée dans un cluster, elle doit être installée sur des volumes du groupe de clusters (Microsoft server cluster) ou paquet de clusters (HPE Serviceguard) ou groupe de services cluster (Symantec Veritas Cluster Server).

Emplacement recommandé des répertoires de la base de données IDB

Partie de l'IDB	Emplacements sur les systèmes Windows	Emplacements sur les systèmes UNIX	Possibilités de déplacement
Espaces de table (CDB, MMDB)	*données_programme_Data_Protector*\server\db80\idb *données_programme_Data_Protector*\server\db80\jce *données_programme_Data_Protector*\server\db80\pg	/var/opt/omni/server/db80/idb /var/opt/omni/server/db80/jce /var/opt/omni/server/db80/pg	Le chemin du répertoire est fixe, mais le montage d'un volume différent est possible.
Fichiers binaires (DCBF, SMBF)	*données_programme_Data_Protector*\server\db80\dcbf *données_programme_Data_Protector*\server\db80\msg *données_programme_Data_Protector*\server\db80\meta	/var/opt/omni/server/db80/dcbf /var/opt/omni/server/db80/msg /var/opt/omni/server/db80/meta	Les chemins des répertoires peuvent être modifiés. De plus, des volumes séparés peuvent être montés.
Fichiers journaux	*données_programme_Data_*	/var/opt/omni/server/db80/pg/pg_xlog_archive	Le chemin du répertoire est

archivés	*Protector* \server\db80\pg\pg_xlog_archive		fixe, mais le montage d'un volume différent est possible.
Fichier de récupération de l'IDB	*données_programme_Data_Protector* \server\db80\logfiles\rlog	/var/opt/omni/server/db80/logfiles/rlog	La copie du fichier peut être située là où vous le souhaitez.



Considérations de robustesse

- La partie centrale de l'IDB, la CDB (objets, positions) et la MMDB, est essentielle au fonctionnement de Data Protector.
- Les parties DCBF et SMBF de l'IDB ne sont pas requises pour les opérations de base de Data Protector, comme la sauvegarde et la restauration. Cependant, si elles ne sont pas présentes, les restaurations deviennent moins pratiques (pas de navigation de noms de fichier) et les messages de session sont perdus.
- Si le fichier de récupération de l'IDB et les fichiers journaux archivés venaient à être perdus, le fonctionnement normal ne serait pas affecté, mais la restauration de l'IDB deviendrait beaucoup plus difficile et la réexécution des données d'IDB générées depuis la dernière sauvegarde de l'IDB serait impossible. A la place, il faudra réimporter le support utilisé.

Configuration de la sauvegarde de la base de données IDB

L'une des étapes essentielles de la gestion d'une cellule HPE Data Protector consiste à configurer la sauvegarde de l'IDB elle-même. La tâche la plus importante que vous pouvez faire pour vous préparer à

un sinistre est d'effectuer la sauvegarde de l'IDB régulièrement. En cas de sinistre pour le Gestionnaire de cellule, la récupération hors ligne de cette base sera essentielle pour pouvoir restaurer d'autres données sauvegardées.

Pour créer une spécification de sauvegarde d'IDB, sélectionnez **Base de données interne** dans la fenêtre de navigation du contexte de sauvegarde, et suivez la procédure de sauvegarde standard. Pour plus d'informations, voir Création d'une spécification de sauvegarde.

Conseils pour la préparation et l'exécution d'une spécification de sauvegarde de l'IDB

Pour configurer la sauvegarde de l'IDB, nous vous recommandons de prendre en compte les points suivants :

- Planifiez une exécution au moins quotidienne de la sauvegarde de l'IDB. Ceci vous permet de toujours disposer d'une sauvegarde actuelle de l'IDB. Planifiez son exécution lorsque l'activité du Gestionnaire de cellule est réduite.

  > **ATTENTION :**
  > Sauvegardez toujours la base de données interne après toute modification dans la configuration d'IDB, par exemple, après avoir changé le mot de passe du service de base de données interne et le compte utilisateur du serveur d'application. Sinon, vous risquez de ne plus pouvoir restaurer correctement l'IDB en ligne et hors ligne.

- Le choix du périphérique et des supports utilisés pour la sauvegarde de l'IDB peut avoir un impact significatif sur la facilité ou la difficulté, ou la possibilité d'effectuer une restauration d'IDB après un sinistre.
  - L'utilisation d'un périphérique pouvant être configuré avec la configuration automatique peut grandement simplifier sa configuration.
  - Si vous utilisez un périphérique de bibliothèque de stockage, vérifiez qu'il est sur un lecteur de disque différent que celui contenant l'IDB.
  - Dans la mesure du possible, utilisez un périphérique connecté en local au Gestionnaire de cellule.
  - N'utilisez pas de bibliothèque de fichiers, car il est impossible d'importer des supports de bibliothèque de fichiers dans une bibliothèque de fichiers.
  - L'importation d'un support StoreOnce Software (SOS) peut être complexe, aussi utilisez uniquement un périphérique SOS pour la sauvegarde de l'IDB si vous avez documenté et testé l'importation du support SOS. Effectuez la sauvegarde de l'IDB en utilisant un pool de supports séparé, sur un support de sauvegarde séparé et sur un périphérique de sauvegarde dédié.
  - Veillez à identifier les supports à utiliser pour la sauvegarde de l'IDB. Vous pouvez configurer un **rapport sur les supports de session** afin d'être informé sur les supports utilisés pour la sauvegarde. Ce rapport simplifie beaucoup une éventuelle restauration.
- Définissez la protection des données et du catalogue de sorte à avoir suffisamment de copies de votre sauvegarde d'IDB pour répondre à vos besoins professionnels.

- Sauf si cela est absolument nécessaire, ne désactivez pas le contrôle automatique de la cohérence de l'IDB. L'option de sauvegarde Vérifier la base de données interne qui contrôle la vérification de la cohérence est sélectionnée par défaut.
- Pour améliorer la confidentialité de vos données, il est possible d'utiliser le cryptage avec les sauvegardes de l'IDB. Une sauvegarde de l'IDB comprend la banque de clés.

  > **REMARQUE :**
  > Vous devez posséder une clé de cryptage active avant de démarrer une sauvegarde cryptée de l'IDB, car il est impossible de créer des clés pendant la sauvegarde.
  > Lors d'une sauvegarde d'IDB cryptée, les clés de cryptage sont automatiquement exportées vers le fichier IDB `IDBClientName-keys.csv` situé dans le répertoire par défaut des clés de cryptage exportées HPE Data Protector.
  > Vous devez faire particulièrement attention à la clé après la sauvegarde. En cas de sinistre, la clé est nécessaire pour une restauration. Après l'exécution de la sauvegarde d'IDB cryptée, copiez la clé correspondante utilisée dans un endroit très sûr.

- Le choix du périphérique et des supports utilisés pour la sauvegarde de l'IDB peut avoir un impact significatif sur la facilité ou la difficulté, ou la possibilité d'effectuer une restauration d'IDB après un sinistre. L'importation d'un support StoreOnce Software (SOS) peut être complexe, aussi utilisez uniquement un périphérique SOS pour la sauvegarde de l'IDB si vous avez documenté et testé l'importation du support SOS. Effectuez la sauvegarde de l'IDB en utilisant un pool de supports séparé, sur un support de sauvegarde séparé et sur un périphérique de sauvegarde dédié.

  > **REMARQUE : Remarque** : Les sauvegardes IDB sur le support logiciel StoreOnce (SOS) qui sont importées après la récupération après sinistre ne sont pas supportées.

- Il est fortement recommandé de documenter et de tester vos procédures de restauration d'IDB DP.

Maintenance de la base de données interne

A propos de la maintenance de la base de données IDB

Si vous avez configuré les notifications et les rapports de la base de données interne les tâches de maintenance à effectuer vous seront signalées. Ces tâches dépendent de la situation dans laquelle se trouve l'IDB.

Situation	Vous pouvez être informé par[1]	Opérations à effectuer
Mémoire insuffisante pour l'IDB	La notification Espace IDB insuffisant	Augmentez la taille de l'IDB Réduisez la croissance de l'IDB Réduisez la taille de l'IDB
Vous souhaitez vérifier la taille de l'IDB	Le rapport sur la taille de l'IDB	Vérifiez la taille de l'IDB

L'IDB ne fonctionne pas correctement, elle est peut-être endommagée	La notification IDB endommagée	Vérifiez la cohérence de l'IDB

[1] Les notifications et les rapports ne s'affichent que s'ils ont été configurés.

> **REMARQUE :**
> HPE recommande de vérifier régulièrement le journal d'événements de Data Protector et d'y rechercher les événements IDB éventuels. Un administrateur peut envisager de configurer des notifications par e-mail afin de susciter une réaction rapide, le cas échéant.

Croissance et performances de la base de données interne

A propos de la croissance et des performances de la base de données IDB

La configuration et la maintenance de la base de données interne exigent de bien comprendre les facteurs ou les paramètres clés qui déterminent ses performances et sa croissance.

Les informations de cette section s'appliquent aux sauvegardes de systèmes de fichiers et illustrent le pire scénario (croissance de l'IDB la plus forte et la plus rapide). Si vous réalisez une sauvegarde d'image disque, une intégration d'application ou une sauvegarde NDMP, seule une petite quantité de données est stockée dans l'IDB.

Facteurs clés de la croissance de l'IDB

La croissance de l'IDB dépend de l'environnement et des paramètres Data Protector définissant le niveau de détails et d'historique que Data Protector doit conserver pour permettre l'exploration et la recherche de fichiers.

Facteurs clés	Effet sur la croissance de l'IDB
Détails sur les fichiers et taille de l'environnement	Data Protector peut effectuer un suivi de chaque fichier et de chaque version du fichier. Ceci signifie qu'au cours de chaque sauvegarde, un enregistrement de nom de fichier (jusqu'à 100 octets) est stocké dans la partie des DCBF pour chaque fichier sauvegardé.
Fréquence des sauvegardes (complètes)	Plus les sauvegardes sont nombreuses, plus il y a d'informations stockées dans l'IDB. Si les variations du système de fichiers sont peu importantes, seule la partie des DCBF augmente.
Nombre de copies d'objets	Plus vous créez de copies et de miroirs d'objets, plus la quantité d'informations stockée dans l'IDB augmente. Pour les copies d'objet et les miroirs d'objet, la base IDB stocke les mêmes informations que pour les objets sauvegardés.

Facteurs clés des performances de l'IDB

Facteurs clés	Effet sur la charge et les performances de l'IDB pendant la sauvegarde
Nombre de lecteurs parallèles	Le nombre de lecteurs (de bande) utilisés en parallèle influe sur la charge de l'IDB. Par exemple, l'utilisation de 10 lecteurs en parallèle pour 10 sessions de sauvegarde, ou de 10 lecteurs en parallèle pour 5 sessions correspond pratiquement à la même charge pour la base de données. Chaque nouveau lecteur représente une autre source de catalogues de fichiers à stocker dans la base de données.
Taille de fichier moyenne	En cas de sauvegarde de petits fichiers, les catalogues de fichiers sont générés plus vite et la charge pour l'IDB est donc plus importante.
Performances des disques de l'IDB	Au cours de la sauvegarde, la principale activité de Data Protector consiste à lire et à écrire sur les disques. Par conséquent, la vitesse du disque (sous-système) utilisé sur le Gestionnaire de cellule pour l'IDB peut agir sur les performances de l'opération.

Paramètres clés des performances et de la croissance de l'IDB

Paramètre clé	Effet sur la croissance de l'IDB	Effet sur les performances de l'IDB
Niveau de journalisation	Définit la quantité de données relatives à des fichiers et à des répertoires qui est écrite dans l'IDB, et l'espace de stockage requis.	Permet d'explorer plus facilement les données à restaurer.
Protection de catalogue	Permet de définir le temps pendant lequel les informations concernant les données sauvegardées (noms et versions de fichier) sont conservées dans l'IDB (base de données interne). Si la protection du catalogue arrive à expiration, les données ne sont pas immédiatement supprimées de l'IDB. Elles sont supprimées le jour même si l'ensemble de la protection du catalogue pour toutes les données du support expire.	Aucune.

La croissance réelle de l'IDB varie selon la durée de la protection du catalogue (période relativement courte, identique à celle utilisée pour la protection des données) et le niveau de journalisation effectif. La croissance significative de l'IDB dure jusqu'à l'expiration de la protection du catalogue. La croissance s'avère ensuite réduite et déterminée par celle de l'environnement de sauvegarde.

Incidence du niveau de journalisation sur la base de données IDB

Les différents paramètres de niveau de journalisation ont une incidence sur la croissance de la base de données interne, sur la facilité d'exploration des systèmes de fichiers à restaurer, et, dans certains cas, sur les performances des sauvegardes.

Les informations fournies ci-dessous concernent les sauvegardes de systèmes de fichiers. Si vous réalisez une sauvegarde d'image disque, de base de données en ligne ou de NDMP, seule une petite quantité de données est stockée dans l'IDB.

Pas de journalisation	Seules les informations sur l'objet sont stockées, généralement 2 Ko par objet du système de fichiers.
Journaliser répertoires	Identique à **Pas de journalisation**, avec 30 octets supplémentaires stockés par répertoire sauvegardé.
Fichiers journal	Identique à **Répertoires de journalisation**, avec 12 octets supplémentaires stockés par répertoire sauvegardé.
Journaliser tout	Identique à **Fichiers journaux**, avec 18 octets supplémentaires stockés par répertoire sauvegardé.

Incidence de la protection de catalogue sur la base de données IDB

La plus grande partie de la base de données interne est proportionnelle à la période de protection du catalogue et au niveau de journalisation choisi. Plus le nombre de sauvegardes effectuées est important au cours de la période de protection du catalogue, plus les données accumulées dans l'IDB sont nombreuses. En d'autres termes, les données nécessaires pour stocker chaque version de fichier sont multipliées par le nombre de versions de fichier sauvegardées au cours de la période de protection.

Une fois la protection de catalogue expirée, les informations ne sont pas immédiatement supprimées de l'IDB. Data Protector les supprime automatiquement une fois par jour. Les informations de l'IDB étant organisées par support, elles ne sont supprimées que lorsque la protection de catalogue expire pour tous les objets du support. Dans ce cas, l'espace occupé par le fichier binaire DC est libéré.

Il est recommandé de paramétrer la protection du catalogue afin d'y inclure au moins la dernière sauvegarde complète. Vous pouvez par exemple la définir sur 8 semaines pour les sauvegardes complètes et sur une semaine pour les sauvegardes incrémentales.

Estimation de la taille de la base de données IDB

Si vous effectuez principalement des sauvegardes de systèmes de fichiers, la base de données interne (IDB) peut dans certaines conditions atteindre une taille significative (plusieurs téraoctets). Si vous réalisez des sauvegardes d'images de disque ou de bases de données en ligne, l'IDB ne devrait pas dépasser plusieurs gigaoctets.

Maintenance des répertoires DC

L'IDB permet d'inscrire plusieurs répertoires à des fins de stockage des fichiers binaires DC (DCBF). Les fichiers binaires DC peuvent ainsi être distribués sur un nombre plus élevé de disques ou de volumes. Par défaut, il existe cinq répertoires nommés `dcbf0` à `dcbf4`.

Chaque répertoire DCBF inclut plusieurs paramètres de configuration :

- Séquence d'allocation
- Chemin d'accès
- Taille maximum
- Nombre maximum de fichiers
- Espace minimal

  Pour plus d'informations sur les paramètres de configuration, reportez-vous au Aide de HPE Data Protector.

Lorsqu'il ne s'avère pas nécessaire de créer un nouveau fichier binaire, la procédure d'allocation DCBF est effectuée par Data Protector :

1. Dans la liste de tous les répertoires DC possibles, Data Protector élimine ceux qui ont été désactivés ou qui sont manquants. Notez que dans le cas d'un répertoire DC manquant, un événement `IDBCorrupted` est généré.

   Tous les répertoires DC complets ne sont pas pris en compte. Un répertoire DC est dit complet si au moins l'une des conditions suivantes est vraie :

   ```
   Maximum size - Current size < Low space
   ```

   ```
   Free disk space < Low space
   ```

   ```
   Maximum files <= Current files
   ```
2. Un ensemble d'algorithmes pouvant être sélectionnés par l'utilisateur (option globale `DCDirAllocation`) sélectionne le répertoire DC effectif.
   - `Fill in sequence`

     Data Protector crée un nouveau fichier binaire DC dans le premier répertoire DC non plein qui figure dans la séquence configurée.

   - `Balance size`

     Data Protector sélectionne le répertoire DC qui contient (proportionnellement à la limite effective de la taille totale) la taille de fichiers DC la plus réduite. La valeur minimale est sélectionnée pour la valeur suivante :

     ```
     (Maximum size - Current size - Low space) / (Maximum size - Low space)
     ```

   - `Balance number`

     Data Protector sélectionne le répertoire DC qui contient (proportionnellement à la limite effective du nombre de fichiers) la taille de fichiers binaires DC la plus réduite. La valeur minimale est sélectionnée pour la valeur suivante :

     ```
     Current files / Maximum files
     ```

Voir les options globales `DCDirAllocation` et `MaxDCDirs` qui influent sur le comportement des DCBF :

Vérification de la taille de la base de données IDB

Vous pouvez vérifier la taille actuelle des parties de la base de données interne à l'aide de l'interface utilisateur graphique de Data Protector.

De plus, si ces éléments sont configurés, le rapport sur la taille de l'IDB ainsi que les notifications Espace IDB insuffisant fournissent des informations sur la taille de l'IDB.

Procédure

1. Dans la liste de contexte, cliquez sur **Base de données interne**.
2. Dans la fenêtre de navigation, développez l'élément **Utilisation**. Les éléments de l'IDB suivant sont affichés : Base de données catalogue, Base de données de gestion des supports, Fichiers binaires de catalogue des détails, Fichiers binaires de messages de session et Fichiers binaires d'intégrations sans serveur.

   L'option Fichiers binaires d'intégrations sans serveur fait référence à une fonctionnalité qui n'est plus prise en charge dans la version installée de HPE Data Protector.
3. Pour vérifier la taille de l'IDB, affichez les propriétés des parties de la base et de leurs enregistrements :
   - Cliquez avec le bouton droit sur un élément de l'IDB, **Base de données catalogue** par exemple, puis sélectionnez **Propriétés** pour afficher l'occupation disque de la partie de la base correspondante. L'occupation disque indique la quantité d'espace disque utilisée par la partie de l'IDB sélectionnée. Cliquez sur l'onglet **Statistiques d'enregistrements** pour afficher les statistiques de tous les enregistrements de cette partie de la base.
   - Pour vérifier l'espace qu'occupe un répertoire DC, développez **Fichiers binaires de catalogue des détails**, double-cliquez sur le répertoire DC, puis sélectionnez l'onglet **Occupation disque**.

Réduction de la croissance de la base de données IDB

Vous pouvez ralentir la croissance de la base de données interne en diminuant les paramètres de niveau de journalisation et de protection de catalogue des spécifications de sauvegarde, de copie d'objets et de consolidation d'objet. Ces opérations n'affectent pas la taille actuelle de l'IDB, mais sa croissance ultérieure.

La diminution du niveau de journalisation limite la possibilité d'exploration lors de la restauration.

La diminution de la protection de catalogue rend impossible l'exploration de certaines restaurations (à savoir, celles provenant de sauvegardes ayant dépassé cette protection).

Les procédures suivantes décrivent la modification de ces paramètres dans une spécification de sauvegarde.

Réduction du niveau de journalisation

En réduisant les paramètres du niveau de journalisation pour une spécification de sauvegarde, vous réduisez la quantité de données (fichiers/répertoires) stockées dans l'IDB (**Journaliser tout** -> **Journaliser fichiers** -> **Journaliser répertoires** -> **Pas de journalisation**).

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécifications de sauvegarde**, puis le type de spécification de sauvegarde (par exemple **Système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez deux fois sur la spécification de sauvegarde dont vous souhaitez modifier le niveau de journalisation, puis sélectionnez l'onglet **Options**.
4. Dans la page de propriétés Options, cliquez sur le bouton **Avancé** (sous **Options du système de fichiers**).
5. Cliquez sur l'onglet **Autre**, puis sous **Journalisation**, modifiez le niveau de journalisation.
6. Cliquez sur **OK** pour appliquer la configuration.

Réduction du catalogue expirée

La réduction de la protection de catalogue ne s'applique qu'aux informations de l'IDB (exploration des restaurations). Ces informations sont toujours stockées sur les supports.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécifications de sauvegarde**, puis le type de spécification de sauvegarde (par exemple **Système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez deux fois sur la spécification de sauvegarde dont vous souhaitez modifier la protection de catalogue, puis sélectionnez l'onglet **Options**.
4. Dans la page de propriétés Options, cliquez sur le bouton **Avancé** (sous **Options du système de fichiers**).
5. Cliquez sur l'onglet **Options** et, sous **Protection de catalogue**, modifiez la protection de catalogue.
6. Cliquez sur **OK** pour appliquer la configuration.

Réduction de la taille de la base de données IDB

Vous pouvez réduire la taille actuelle de la base de données interne en modifiant les paramètres de protection de catalogue pour l'ensemble d'une session de sauvegarde, de copie d'objets ou de consolidation d'objets (tous les objets de la session) ou seulement pour des objets spécifiques.

La diminution de la protection de catalogue rend impossible l'exploration de certaines restaurations (à savoir, celles provenant de sauvegardes ayant dépassé cette protection).

Cette opération n'a aucun effet sur la croissance ultérieure de l'IDB.

La réduction s'applique dans les cas suivants :

- Si la protection de catalogue est supprimée de tous les objets d'un support.
- Une fois par jour (par défaut à midi), lorsque Data Protector supprime automatiquement les données obsolètes de l'IDB. Vous pouvez indiquer l'heure à l'aide de l'option globale `DailyMaintenanceTime`. Utilisez la notation horaire européenne.

  Vous pouvez démarrer la purge immédiatement en exécutant la commande `omnidbutil -purge -dcbf`. Pour obtenir des informations sur la suppression d'autres éléments obsolètes de l'IDB, consultez la page `omnidbutil` du manuel ou le *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

La modification de la protection de catalogue ne s'applique qu'aux informations d'exploration des restaurations de l'IDB. Ces informations sont toujours stockées sur les supports. Ainsi, si vous exportez un support et le réimportez, Data Protector lit à nouveau les informations sur la protection de catalogue à partir du support.

Modification de la protection de catalogue pour une session

La modification de la protection d'une session de sauvegarde s'applique à tous les objets sauvegardés dans cette session.

Procédure

1. Dans la liste de contexte, cliquez sur **Base de données interne**.
2. Dans la fenêtre de navigation, développez l'élément **Sessions**.
3. Cliquez avec le bouton droit sur les sessions dont vous souhaitez modifier la protection, puis choisissez **Changer protection de catalogue**.
4. Indiquez la nouvelle protection de catalogue des sessions, puis cliquez sur **Terminer** pour appliquer vos modifications.

Modification de la protection de catalogue pour un objet

La modification de la protection d'un objet donné s'applique à cet objet quelle que soit la session au cours de laquelle il a été sauvegardé.

Procédure

1. Dans la liste de contexte, cliquez sur **Base de données interne**.
2. Dans la fenêtre de navigation, développez l'élément **Objets**.
3. Cliquez avec le bouton droit sur les objets dont vous souhaitez modifier la protection, puis choisissez **Changer protection du catalogue**.
4. Indiquez la nouvelle protection de catalogue des objets, puis cliquez sur **Terminer** pour appliquer vos modifications.

Extension de la taille de la base de données IDB

En raison du manque d'espace disque disponible pour la partie des détails de l'IDB (noms, les versions et métadonnées des objets sauvegardés), vous devrez peut-être étendre la base de données interne en

créant des répertoires DC ou en augmentant la capacité des répertoires existants.

Augmentation de la capacité des répertoires DC

Vous pouvez reconfigurer un répertoire DC existant en modifiant ses options Séquence d'allocation, Taille maximum, Nombre maximum de fichiers ou Espace minimum. Notez que le nombre et la taille totale actuelle des fichiers du répertoire DC choisi peuvent limiter la plage d'ajustement.

Procédure

1. Dans la liste de contexte, cliquez sur **Base de données interne**.
2. Dans la fenêtre de navigation, développez l'élément **Utilisation** puis **Fichiers binaires de catalogue des détails**.
3. Cliquez avec le bouton droit de la souris sur le chemin du répertoire DC choisi, puis sélectionnez **Propriétés**.
4. Dans la zone de résultats, modifiez les options disponibles, si nécessaire.
5. Cliquez sur **Terminer** pour appliquer vos modifications.

Vérification de la cohérence de la base de données IDB

Le contenu de la base de données interne doit être correct d'un point de vue logique. En d'autres termes, les parties de l'IDB doivent être cohérentes et en ordre. Vous pouvez effectuer des contrôles de cohérence manuellement pour des parties spécifiques et pour l'IDB entière.

Data Protector vérifie la cohérence de l'IDB par défaut avant la sauvegarde de l'IDB (vérification rapide). Cela est extrêmement important pour la récupération de l'IDB et des données sauvegardées en cas de sinistre sur le Gestionnaire de cellule.

Type de contrôle d'IDB	Ce qui est vérifié	Commande
Vérification rapide de l'IDB	Le noyau (MMDB et CDB), les noms de fichiers et la vérification simple des parties DCBF.	`omnidbcheck -quick`
Vérification simple de la partie DCBF	Si les fichiers binaires DC existent ou non et quelle est leur taille.	`omnidbcheck -bf`
Vérification complète de la partie DCBF	La cohérence des positions des supports et des fichiers binaires DC.	`omnidbcheck -dc`
Vérification de la partie SMBF	Présence des fichiers binaires de messages de session.	`omnidbcheck -smbf`
Contrôle de cohérence des supports	La cohérence des supports. Répertorie également les noms de support incohérents en cas de problème de cohérence de support.	`omnidbcheck -media_consistency`

Contrôle de cohérence du schéma	La cohérence du schéma de l'IDB. Détecte également toutes les modifications au schéma depuis sa première création lors de l'installation de Data Protector.	`omnidbcheck -schema_consistency`
Contrôle de cohérence de la base de données	La cohérence de la base de données. Répertorie également les erreurs en cas de problème de cohérence de la base de données.	`omnidbcheck -database_consistency`
Vérification complète de l'IDB	Toutes les vérifications hors SMBF sont effectuées.	`omnidbcheck -extended`

Déplacement de la base de données IDB vers un autre Gestionnaire de cellule

Vous pouvez déplacer la base de données interne vers un autre Gestionnaire de cellule exécuté sur le même système d'exploitation.

Dans un premier scénario, pour lequel vous effectuez la restauration de l'IDB depuis un périphérique de sauvegarde sur un client Data Protector, procédez comme suit :

Procédure

1. Préparez un périphérique de sauvegarde *PériphériquePréparé* sur le client Data Protector*client.société.com*.
2. Exécutez la sauvegarde de l'IDB avec l'appareil de sauvegarde PériphériquePréparé.
3. Préparez le nouveau Gestionnaire de cellule Data Protector sur l'hôte *cmb.société.com* : installation propre.
4. Exportez le client *client.société.com* depuis le Gestionnaire de cellule sur l'hôte *cma.société.com*.
5. Importez le client *client.société.com* vers le nouveau Gestionnaire de cellule sur l'hôte *cmb.société.com*.
6. Importez le périphérique de sauvegarde *PériphériquePréparé* sur le nouveau Gestionnaire de cellule.
7. Exécutez la restauration de l'IDB depuis le périphérique de sauvegarde *PériphériquePréparé*.
8. Arrêter les services de HPE Data Protector.
9. Pour tous les mots de passe (`mot de passe de magasin de clés`, `mot de passe truststore`, `mot de passe ssl`, et `le mot de passe ca-certificate`) situés dans le fichier de configuration `standalone.xml`, utilisez le `Mot de passe du magasin de clé` depuis le fichier de configuration `webservice.properties`.

   Ces fichiers de configuration sont disponibles dans les emplacements suivants :

   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`

10. Démarrer les services de HPE Data Protector.
11. Importez des clients du Gestionnaire de cellule d'origine vers le nouveau Gestionnaire de cellule.

> **IMPORTANT :**
> Chaque client doit avoir été exporté depuis le Gestionnaire de cellule d'origine au préalable.

12. Reconnectez l'interface graphique au nouveau Gestionnaire de cellule.

Dans un deuxième scénario, pour lequel vous effectuez la restauration de l'IDB depuis un périphérique de sauvegarde sur le Gestionnaire de cellule d'origine, procédez comme suit :

Procédure

1. Préparez un périphérique de stockage *PériphériquePréparé* sur le Gestionnaire de cellule d'origine.
2. Exécutez la sauvegarde de l'IDB avec l'appareil de sauvegarde PériphériquePréparé.
3. Préparez le nouveau Gestionnaire de cellule Data Protector sur l'hôte *cmb.société.com* : installation propre.
4. Exportez le périphérique de sauvegarde *PériphériquePréparé* depuis le Gestionnaire de cellule d'origine.
5. Importez le périphérique de sauvegarde *PériphériquePréparé* vers le nouveau Gestionnaire de cellule sur l'hôte *cmb.société.com*.
6. Exécutez la restauration de l'IDB depuis le périphérique de sauvegarde PériphériquePréparé.
7. Arrêter les services de HPE Data Protector.
8. Pour tous les mots de passe (`mot de passe de magasin de clés`, `mot de passe truststore`, `mot de passe ssl`, et `le mot de passe ca-certificate`) situés dans le fichier de configuration `standalone.xml`, utilisez le `Mot de passe du magasin de clé` depuis le fichier de configuration `webservice.properties`.

   Ces fichiers de configuration sont disponibles dans les emplacements suivants :

   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`

9. Démarrer les services de HPE Data Protector.
10. Importez des clients du Gestionnaire de cellule d'origine vers le nouveau Gestionnaire de cellule.

> **IMPORTANT :**
> Chaque client doit avoir été exporté depuis le Gestionnaire de cellule d'origine au préalable.

11. Reconnectez l'interface graphique au nouveau Gestionnaire de cellule.

Personnalisation des options globales de Data Protector

Dans le fichier des options globales Data Protector, vous pouvez modifier les valeurs des options globales ou en ajouter.

Conditions préalables

- Votre compte utilisateur doit être membre d'un groupe d'utilisateurs Data Protector `Admin`.

Définition des options globales à l'aide de l'interface utilisateur graphique

Procédure

Pour définir les options globales à l'aide de l'interface utilisateur graphique :

1. Dans la liste de contexte, cliquez sur **Base de données interne**.
2. Dans la fenêtre de navigation, sous **Base de données interne**, cliquez sur **Options globales**.

   La zone de résultats affiche le tableau **Data Protector Options globales**, composé de six colonnes :
   - Groupe - représente la section contextuelle à laquelle l'option appartient.
   - Utilisée - indique l'état d'une option. Les options sélectionnées sont actives, tandis que la case à cocher vide indique les options inactives dans le fichier d'options globales.
   - Nom
   - Origine - indique le fichier à partir duquel l'option est chargée.
   - Valeur - représente la valeur actuelle de l'option.
   - Description - vous indique comment utiliser l'option.
3. Pour modifier une option, dans la colonne Valeur du panneau des résultats, cliquez sur la valeur à modifier, cliquez sur l'icône d'édition  , puis entrez une nouvelle valeur. Cliquez sur **Enregistrer** pour enregistrer l'option.

   Pour ajouter une option, cliquez sur l'icône Ajouter  , définissez les paramètres de l'option dans la boîte de dialogue, puis cliquez sur **Ajouter**.
4. Dans le bas de la fenêtre des résultats, cliquez sur l'icône Enregistrer  .

Vous pouvez également modifier plusieurs lignes avant d'enregistrer le tableau.

Pour modifier l'apparence du tableau, utilisez les filtres des titres.

Si un problème survient lors du processus d'enregistrement, une copie du fichier original des options globales, nommée `global.old`, est créée dans le dossier des options globales.

Personnalisation d'options en éditant le fichier global

Outre l'utilisation de l'interface utilisateur, vous pouvez modifier le fichier `global` dans un éditeur de texte pour définir les options globales Data Protector.

> **ATTENTION :**
> HPE recommande d'utiliser l'interface graphique pour définir les options globales, car vous validez les modifications lors de l'enregistrement et réduisez les risques de problèmes liés à des valeurs hors plage ou non valides, à la suppression accidentelle et aux erreurs typographiques ou orthographiques.

Procédure

1. Ouvrez un éditeur de texte quelconque
2. Dans l'éditeur de texte, ouvrez le fichier `global`, situé dans le répertoire de configuration du serveur Data Protector par défaut, dans le sous-répertoire `options`.
3. Pour activer une option, supprimer la marque # de son nom et définissez-la sur la valeur souhaitée.
4. Enregistrez le fichier au format Unicode.

Configuration des rapports de la base de données IDB

Configurez les rapports de la base de données interne pour être informé de l'échéance des tâches de maintenance à effectuer (par exemple, extension de la taille de l'IDB ou réduction de sa croissance).

Rapports de l'IDB

Rapport	Vous indique...
Rapport sur la taille de la base de données interne	... la taille des différentes parties de l'IDB.

Configuration des notifications de la base de données IDB

Configurez les notifications de la base de données interne pour être informé de l'échéance de chaque tâche de maintenance à effectuer (par exemple, purge de l'IDB, extension de sa taille, vérification de sa cohérence, etc.).

Notifications de l'IDB

Notification	Vous indique...

Peu d'espace dans la base de données interne	... que l'IDB manque d'espace.
Limites IDB	... si une partie quelconque des la MMDB ou de la CDB a atteint sa limite.
Sauvegarde IDB requise	... si une sauvegarde de l'IDB ne se produit pas fréquemment, ou si les sauvegardes de l'IDB incrémentales successives sont trop nombreuses.

Restauration de la base de données IDB

Vous pouvez restaurer la base de données interne (IDB) depuis une image de sauvegarde créée dans la procédure de sauvegarde d'IDB standard. Si l'IDB est corrompue, vous ne pouvez pas utiliser cette procédure de restauration, mais vous devez suivre une des méthodes de récupération d'IDB.

Pour restaurer la base de données interne, procédez comme suit :

- Restauration de la base de données IDB

Lors de la restauration depuis une sauvegarde d'IDB cryptée, des étapes supplémentaires sont requises avant la restauration effective :

- Préparation de la restauration d'IDB à partir d'une sauvegarde cryptée

Restauration de la base de données IDB

Lors de la restauration de la base de données interne, les éléments de base de l'IDB (CDB, MMDB, SMBF) peuvent uniquement être restaurés vers un emplacement différent de l'original, lorsque les données de configuration du Gestionnaire de cellule et les fichiers binaires du catalogue de détails (DCBF) de l'IDB peuvent être restaurés vers l'emplacement d'origine ou un autre emplacement.

Conditions préalables

- En fonction de la taille de l'image de sauvegarde de votre base de données interne, vérifiez qu'il y a assez d'espace disque libre sur le Gestionnaire de cellule.

Limites

L'utilisation de l'IDB restaurée comme nouvelle IDB avec l'option "utiliser la base de données restaurée comme nouvelle base de données interne" n'est pas prise en charge sur la configuration de cluster SG. Vous pouvez définir la variable omnirc `OB2SGENABLED`, qui fournit la procédure pour utiliser l'IDB restaurée comme nouvelle IDB dans le rapport de session. Lorsque vous définissez la variable omnirc, vous verrez le message suivant dans le rapport de session :

```
[Warning] From: OB2BAR_POSTGRES_BAR@<nom hôte> "DPIDB"  Time: <date heure>

[175:316] Le remplacement automatique de la base de données interne dans un
environnement de clusters n'est pas pris en charge.
```

Cliquez sur le numéro d'erreur dans le message pour plus d'informations sur la procédure à suivre pour utiliser l'IDB restaurée comme une nouvelle IDB.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, développez **Restaurer des objets**, puis **Base de données interne**.
3. Développez le Gestionnaire de cellule depuis là où l'IDB a été sauvegardée, et cliquez sur **Base de données interne**.
4. Sur la page de propriétés Base de données interne, pour restaurer les éléments de base de la base de données interne, laissez l'option **Restaurer la base de données interne** cochée. Les éléments de base de l'IDB sont la base de données de catalogue (CDB), la base de données de gestion des supports (MMDB) et les fichiers binaires de messages de session (SMBF). Spécifiez le port temporaire à utiliser pour le service de base de données interne lors de la restauration, et l'emplacement auquel les éléments de base de l'IDB doivent être restaurés.

   De plus, décidez si vous souhaitez effectuer la récupération de la base de données interne avec les fichiers journaux archivés et si l'IDB doit être mise en service en tant que nouvelle base de données interne de la cellule.
5. Sélectionnez **Restaurer les fichiers binaires de catalogue** pour restaurer la partie DCBF de l'IDB, et choisissez son emplacement de restauration : origine ou personnalisé.
6. Spécifiez si Data Protector doit restaurer l'IDB à un point spécifique dans le temps qui n'est pas la date de la dernière création d'image de sauvegarde de l'IDB. Dans ce cas, la partie de base de la base de données interne sera restaurée à l'état de la dernière sauvegarde avant la date spécifiée.
7. Sur la page de propriétés **Fichiers de configuration**, choisissez une option pour la restauration des données de configuration du Gestionnaire de cellule. Si ces données sont sélectionnées pour restauration, vous devez aussi spécifier sa version d'objet de sauvegarde, et choisir si Data Protector gérera les fichiers de configuration qui existent encore à l'emplacement d'origine.
8. Sur la page de propriétés **Options**, spécifiez les commandes optionnelles pré et post-exécution pour la session de restauration.
9. Sur la page de propriétés **Périphériques**, faites votre choix concernant les périphériques à utiliser lors de la session.
10. Sur la page de propriétés **Supports**, vérifiez les supports de sauvegarde qui seront utilisés pour la restauration de l'IDB. De façon optionnelle, ajustez les propriétés que Data Protector considérera pendant la session.
11. Dans le menu Actions, sélectionnez **Démarrer la restauration**, ou cliquez sur **Restaurer** dans la fenêtre des résultats.
12. Cliquez sur **Terminer**.

> **IMPORTANT :**
> Après une restauration d'IDB à un point dans le temps, copiez les fichiers spécifiques du répertoire `auditing_IDBRestoreSessionID_NNNNNNNNN` vers le répertoire `auditing` d'origine. Cela rendra les informations d'audit cohérentes avec l'état de l'IDB restaurée. Les journaux d'audit suivants doivent être copiés :
>
> `YYYY_MM_DD.med`

YYYY_MM_DD.obj

YYYY_MM_DD.ses

Dans les noms de fichier ci-dessus, les chaînes *YYYY*, *MM* et *DD* correspondent à la date spécifiée avec l'option **Restaurer jusqu'au** sur la page de propriétés de la base de données interne.

REMARQUE :
Après la restauration, vous voudrez peut-être vérifier la cohérence de l'IDB.

Préparation de la restauration d'IDB à partir d'une sauvegarde cryptée

Lors d'une sauvegarde d'IDB cryptée, les clés de cryptage sont automatiquement exportées vers le fichier IDB `IDB-ClientName-keys.csv` situé dans le répertoire par défaut des clés de cryptage exportées Data Protector.

Avant la restauration de l'IDB, procédez comme suit :

Procédure

1. Transférez le fichier `IDB-ClientName-keys.csv` vers le Gestionnaire de cellule où vous effectuerez la restauration de l'IDB.
2. Importez la clé en exécutant :

   ```
   omnikeytool -import CSVFile
   ```

Le Gestionnaire de cellule utilisera la clé KMS en ligne pour décrypter les données sur le support contenant la sauvegarde de l'IDB.

A propos de la récupération de la base de données IDB

Une récupération de la base de données interne s'avère nécessaire si tout ou partie de ses fichiers ne sont pas disponibles ou sont endommagés.

Il y a trois niveaux de problèmes concernant l'IDB, chacun d'entre eux exigeant une résolution différente :

- Résolution de problèmes au niveau de l'IDB causés par des défauts de configuration du système d'exploitation, tels que des systèmes de fichiers non montés, des problèmes de services de noms, etc.
- Omission ou suppression de parties non centrales (fichiers binaires) de l'IDB qui posent problème. Ceci s'avère possible si le niveau d'altération de l'IDB est identifié comme mineur (l'altération ne se trouve pas dans la partie centrale de l'IDB).
- Récupération complète, à savoir restauration et mise à jour de l'IDB après sa dernière sauvegarde. Ceci s'avère obligatoire si le niveau d'altération de l'IDB est identifié comme critique (l'altération se trouve dans la partie centrale).

Récupération complète (restauration et mise à jour de l'IDB après sa dernière sauvegarde)

La restauration complète se divise en deux phases :

1. Restauration de l'IDB, à savoir sa restitution au dernier état cohérent (disponible).
2. Mise à jour de l'IDB à partir du dernier état cohérent jusqu'au dernier stade où elle était opérationnelle.

Selon le degré de préparation de la récupération avant l'arrivée des problèmes (disponibilité du fichier de récupération de l'IDB, des images de sauvegarde de l'IDB, du périphérique d'origine et des fichiers journaux archivés), la procédure de récupération peut varier. Si vous disposez de tous ces éléments, vous pouvez effectuer la récupération de l'IDB très simplement au moyen d'une procédure automatique guidée.

Présentation des méthodes de récupération de la base de données IDB

Vous disposez de plusieurs méthodes pour récupérer la base de données interne. La procédure de récupération sera différente selon le niveau d'altération identifié, votre configuration et la disponibilité du fichier de récupération de l'IDB, du périphérique de sauvegarde d'origine et des fichiers journaux archivés.

Récupération complète la plus pratique

Cette méthode de récupération vous guide tout au long de la restauration de l'IDB et de la réexécution des fichiers journaux archivés. Si vous ne disposez pas des fichiers journaux archivés, vous pouvez toujours mettre l'IDB à jour en important tous les supports depuis sa dernière sauvegarde.

Niveau d'altération	Type de problème	Situation actuelle	Procédure de récupération
Critique	La totalité de l'IDB est manquante ou la partie centrale est endommagée.	Le fichier de récupération de l'IDB et le périphérique d'origine utilisés pour la sauvegarde de l'IDB sont disponibles.	Dans la mesure du possible, lancez la récupération automatique guidée (restauration de l'IDB et réexécution des journaux). Sinon, suivez l'une des méthodes proposées à la section Autres méthodes de récupération.

Omission (suppression) des parties de l'IDB endommagées

Si le niveau d'altération identifié est mineur (l'altération ne se situe pas au niveau de la partie centrale), vous pouvez omettre (supprimer) les parties manquantes ou endommagées de l'IDB ou effectuer une

récupération complète de la base.

Niveau d'altération	Type de problème	Procédure de récupération
Mineur	Des fichiers binaires DC sont manquants ou endommagés.	Traitement d'altération mineure de l'IDB dans la partie DCBF

Autres méthodes de récupération

Ces méthodes de récupération s'appliquent à des cas particuliers. Supposons que vous souhaitiez récupérer l'ensemble de l'IDB, mais que, pour une raison donnée, vous ne puissiez pas appliquer la méthode de récupération automatique guidée. La récupération consiste à restaurer l'IDB, puis à la mettre à jour.

Restaurer

Situation actuelle	Remarque	Procédure de récupération (restauration de l'IDB)
Le fichier de récupération de l'IDB est disponible, mais le périphérique d'origine n'est pas celui utilisé pour la sauvegarde de la base.	Cette méthode est pratiquement identique à la méthode de récupération automatique guidée, mais elle est moins directive, plus complexe et plus longue.	Restauration de l'IDB avec le fichier de récupération de l'IDB et un autre périphérique
Le fichier de restauration de l'IDB n'est pas disponible.	Cette méthode est pratiquement identique à la méthode de récupération automatique guidée, mais elle est moins directive, plus complexe et plus longue.	Restauration de l'IDB sans le fichier de récupération de l'IDB
Vous souhaitez récupérer l'IDB à partir d'une sauvegarde spécifique (pas la dernière).	Cette méthode ne restitue pas le dernier état de l'IDB.	Restauration de l'IDB à partir d'une session spécifique de l'IDB

Mise à jour de l'IDB depuis sa dernière sauvegarde

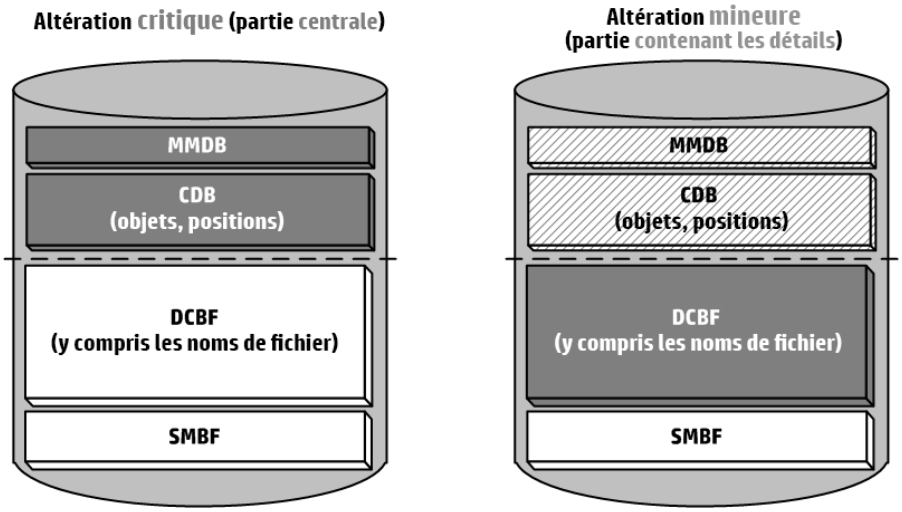
Situation actuelle	Procédure de récupération (mise à jour de l'IDB)
Les fichiers journaux archivés ne sont pas disponibles.	Mise à jour de l'IDB par l'importation de supports

Niveaux d'altération de la base de données IDB

Il existe deux niveaux d'altération de la base de données interne : critique et mineure. Le niveau dépend de la partie de l'IDB affectée par l'altération.

Vous pouvez utiliser la vérification de la cohérence de l'IDB pour identifier la partie endommagée.

La procédure de récupération de l'IDB dépend du niveau d'altération.



Identification du niveau d'altération de la base de données IDB

L'identification du niveau d'altération permet de choisir la méthode de récupération de la base de données interne appropriée.

Procédure

1. Identifiez le niveau d'altération à l'aide de la commande `omnidbcheck -extended`.

   > **REMARQUE :**
   > La vérification étendue peut demander un temps considérable. Au lieu de cela, vous pouvez exécuter des parties de la commande `omnidbcheck`. Par exemple, exécutez la commande `omnidbcheck -connection` pour vous assurer que la connexion à l'IDB est établie.

Une fois le niveau d'altération identifié, suivez la procédure de récupération appropriée.

Récupération automatique guidée (restauration de la base de données IDB et réexécution des fichiers de journal archivés)

La méthode de récupération automatique guidée est la méthode de récupération de la base de données interne la plus pratique. Vous pouvez l'adopter si le fichier de récupération de l'IDB et le périphérique d'origine utilisé pour la sauvegarde de l'IDB ainsi que le support de sauvegarde de l'IDB sont disponibles.

Cette méthode vous guide tout au long de la restauration de l'IDB et de la réexécution des fichiers de journal archivés depuis la dernière sauvegarde de l'IDB. Si les fichiers de journal archivés ne sont pas

disponibles, vous pouvez toujours mettre l'IDB à jour depuis la dernière sauvegarde en important les supports.

La réexécution des journaux de transactions entraîne la mise à jour de la partie centrale de l'IDB. Les fichiers binaires ne sont pas mis à jour et les modifications apportées à ces derniers sont perdues. Les éléments suivants ne sont pas disponibles pour les sauvegardes exécutées entre la dernière sauvegarde et l'altération de l'IDB :

- Messages de session.
- Exploration des versions de fichier (il est possible de restaurer les objets complets). Pour récupérer les modifications, vous devez importer le catalogue sur les supports utilisés par les sauvegardes.

Conditions préalables

- En fonction de la taille de l'image de sauvegarde de votre base de données interne, vérifiez qu'il y a assez d'espace disque libre sur le Gestionnaire de cellule.
- Vérifiez que le Gestionnaire de cellule possède le double de RAM que prescrit par la configuration requise pour l'installation du Gestionnaire de cellule Data Protector dans le document *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*. Si le Gestionnaire de cellule est un système UNIX, vérifiez que son paramètre de noyau `shmmax` est défini sur le double de la valeur requise indiquée dans la même section.
- Montez un disque dont la taille est identique à celle du disque avant le sinistre sur les mêmes répertoires que lors de la sauvegarde de l'IDB (sur les systèmes Windows, les mêmes lettres de lecteur doivent être affectées). Si vous ne pouvez pas effectuer cette opération, suivez la procédure de récupération de l'IDB sur une configuration de disque/volume différente. Vous pouvez utiliser l'option `-preview` de la commande `omnioffl r` pour savoir où les fichiers seront restaurés.
- Installez Data Protector sur le Gestionnaire de cellule et sur le système auquel un périphérique est connecté (de préférence le périphérique utilisé pour la sauvegarde de l'IDB).
- Si l'IDB est installée sous HPE Serviceguard, les commandes suivantes doivent être exécutées sur le nœud actif avant la récupération automatique guidée :
  1. `cmhaltpkg` *`PackageName`*, où *`PackageName`* est le nom du package de cluster Data Protector. Cette commande arrête le package Data Protector et démonte le groupe de volumes Data Protector partagé.
  2. `vgchange -a e /dev/`*`vg_name`*, où *`vg_name`* est le nom du groupe de volumes partagés Data Protector. Cette commande permet d'activer le groupe de volumes partagé Data Protector. Pour afficher les liste des groupes de volumes du système, exécutez la commande `ll /dev/*/group`.
  3. `mount /dev/`*`vg_name`*`/lv_name/`*`MountPoint`*, où *`MountPoint`* est le nom du point de montage pour le groupe de volumes partagés Data Protector. Cette commande permet de monter le groupe de volumes Data Protector partagé.

  Lorsque la récupération automatique guidée est terminée, exécutez la commande `cmrunpkg` *`PackageName`* sur le nœud actif pour démarrer le package Data Protector.
- Si l'IDB est installée sur un serveur de clusters Symantec Veritas, mettez la ressource d'application Data Protectorhors ligne sur le nœud actif avant d'effectuer la récupération automatique guidée.

  Lorsque la récupération automatique guidée est terminée, mettez la ressource d'application Data Protectoren ligne sur le nœud actif pour démarrer le service Data Protector.
- Si l'IDB est installée sur un Microsoft Cluster Server, mettez les groupes de clusters `OOBVS_HPDP_`

AS, OBVS_HPDP_IDB, et OBVS_HPDP_IDB_CP hors ligne à l'aide de l'utilitaire d'administration des clusters et arrêtez le service Inet sur le nœud actif avant d'effectuer la récupération automatique guidée. Une fois la récupération automatique guidée terminée, mettez les groupes de clusters OBVS_HPDP_AS, OBVS_HPDP_IDB, OBVS_HPDP_IDB_CP, et OBVS_MCRS en ligne à l'aide de l'utilitaire de l'Administrateur de clusters, puis redémarrez le service Inet.

Procédure

1. Exécutez la commande omniofflr -idb -autorecover.

   Cette commande lit le fichier de récupération de l'IDB. Si les sauvegardes de l'IDB sont consignées dans le fichier, les services sont arrêtés et la base restaurée. Toutes les options sont générées automatiquement avec les données du fichier de récupération de l'IDB.

   Une fois la restauration terminée, omniofflr vérifie si les journaux de transactions peuvent être exécutés à nouveau. Si les fichiers de journal sont disponibles, vous êtes invité à confirmer leur réexécution. Si cette étape est annulée ou si les fichiers de journal archivés ne sont pas disponibles, vous êtes informé de la méthode pour mettre à jour l'IDB depuis sa dernière sauvegarde par les opérations suivantes :

   - importation de supports ;
   - recherche des fichiers de journal archivés et réexécution ultérieure de ceux-ci.

   Une fois les fichiers de journal réexécutés ou les supports importés pour la mise à jour de l'IDB, cette dernière est normalement restituée dans son intégralité.

Traitement d'une altération mineure de la base de données IDB dans la partie DCBF

Si vous réalisez que la base de données interne présente une altération mineure, cela signifie que certains fichiers binaires DC sont manquants ou endommagés. vous n'êtes pas obligé d'effectuer une récupération complète de l'IDB. Vous pouvez facilement recréer les fichiers binaires en important le catalogue à partir des supports. Choisissez la procédure de récupération en fonction du type d'altération :

Récupération si des fichiers binaires DC sont manquants

Chaque support contient un fichier binaire DC. Si certains de ces fichiers sont manquants, les positions de certains supports désignent des fichiers inexistants. Un message d'erreur s'affiche lors de l'exploration des systèmes de fichiers correspondants.

Procédure

1. A partir des résultats de la commande omnidbcheck -bf, identifiez l'ID du support du fichier binaire manquant. Exécutez la commande omnimm -media_info *medium-id* pour obtenir les autres attributs du support, comme son étiquette et le pool auquel il appartient.
2. Exécutez la commande omnidbutil -fixmpos pour rétablir la cohérence entre les positions de

support (mpos) et les fichiers binaires.

3. Importez le catalogue à partir des supports afin de recréer les fichiers binaires.

Récupération si des fichiers binaires DC sont endommagés

Si certains fichiers binaires DC sont endommagés, vous pouvez les supprimer et les recréer en important les supports avec un niveau de journalisation approprié. A 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.

Procédure

1. A partir des résultats de la commande `omnidbcheck -dc`, identifiez l'ID du support du fichier binaire DC endommagé. Exécutez la commande `omnimm -media_info` *`medium-id`* pour obtenir les autres attributs du support, comme son étiquette et le pool auquel il appartient.
2. Identifiez le fichier binaire DC du support concerné. Les fichiers binaires DC se nomment : *`MediumID_TimeStamp`*`.dat` (dans le `MediumID`, les signes deux-points " : " sont remplacés par des traits de soulignement " _ ").
3. Supprimez les fichiers binaires DC endommagés.
4. Exécutez la commande `omnidbutil -fixmpos` pour rétablir la cohérence entre les positions de support (mpos) et les fichiers binaires.
5. Importez le catalogue à partir des supports afin de recréer les fichiers binaires.

Restauration de la base de données IDB avec le fichier de récupération de l'IDB et un autre périphérique

Utilisez cette procédure pour restaurer la base de données interne si le fichier de récupération de l'IDB est disponible, mais que le périphérique d'origine utilisé pour la sauvegarde de l'IDB est différent de celui utilisé pour la récupération ou que le support est situé sur un emplacement différent.

Conditions préalables

- Montez un disque dont la taille est identique à celle du disque avant le sinistre sur les mêmes répertoires que lors de la sauvegarde de l'IDB (sur les systèmes Windows, les mêmes lettres de lecteur doivent être affectées). Si vous ne pouvez pas effectuer cette opération, suivez la procédure de récupération de l'IDB sur une configuration de disque/volume différente. Vous pouvez utiliser l'option `-preview` de la commande `omnioffl r` pour savoir où les fichiers seront restaurés.
- Dans la mesure du possible, déplacez le fichier `media.log` de l'installation précédente en lieu sûr. Celui-ci contient des informations sur les supports utilisés depuis la dernière sauvegarde de l'IDB. Il vous sera très utile pour mettre à jour l'IDB si les journaux de transactions ne sont pas disponibles.
- Installez Data Protector sur le Gestionnaire de cellule et sur le système auquel un périphérique est connecté (de préférence le périphérique utilisé pour la sauvegarde de l'IDB).
- Si l'IDB est installée sous HPE Serviceguard, les commandes suivantes doivent être exécutées sur le nœud actif avant la récupération automatique guidée :

1. `cmhaltpkg PackageName`, où *PackageName* est le nom du package de cluster Data Protector. Cette commande arrête le package Data Protector et démonte le groupe de volumes Data Protector partagé.
2. `vgchange -a e /dev/vg_name`, où *vg_name* est le nom du groupe de volumes partagés Data Protector. Cette commande permet d'activer le groupe de volumes Data Protector partagé. Pour afficher les liste des groupes de volumes du système, exécutez la commande `ll /dev/*/group`.
3. `mount /dev/vg_name/lv_name/MountPoint`, où *MountPoint* est le nom du point de montage pour le groupe de volumes partagés Data Protector. Cette commande permet de monter le groupe de volumes Data Protector partagé.

Lorsque la récupération automatique guidée est terminée, exécutez la commande `cmrunpkg PackageName` sur le nœud actif pour démarrer le package Data Protector.

- Si l'IDB est installée sur un serveur de clusters Symantec Veritas, mettez la ressource d'application Data Protectorhors ligne sur le nœud actif avant d'effectuer la récupération automatique guidée.

  Lorsque la récupération automatique guidée est terminée, mettez la ressource d'application Data Protectoren ligne sur le nœud actif pour démarrer le service Data Protector.
- Si l'IDB est installée sur un Microsoft Cluster Server, mettez les groupes de clusters `OBVS_HPDP_AS, OBVS_HPDP_IDB,` et `OBVS_HPDP_IDB_CP` hors ligne à l'aide de l'utilitaire d'administration des clusters et arrêtez le service `Inet` sur le nœud actif avant d'effectuer la récupération automatique guidée. Une fois la récupération automatique guidée terminée, mettez les groupes de clusters `OBVS_HPDP_AS, OBVS_HPDP_IDB, OBVS_HPDP_IDB_CP,` et `OBVS_MCRS` en ligne à l'aide de l'utilitaire de l'Administrateur de clusters, puis redémarrez le service `Inet`.

Procédure

1. Exécutez la commande suivante pour créer un fichier texte comportant les options de la tâche de restauration :

   ```
   omnioffl r -idb -autorecover -save C:\TEMP\restjob.txt -skiprestore -logview
   ```

   La commande `-logview` spécifiée dresse la liste des fichiers de journal archivés, avec les ID de session. Gardez en mémoire le nom du premier fichier de journal archivé de la session à restaurer car il vous sera nécessaire pour mettre à jour l'IDB après la restauration. Par exemple, pour le résultat `2013/02/09-2 AAAAAAH`, gardez en mémoire le nom du premier fichier de journal archivé `AAAAAAH` afin de restaurer la `2013/02/09-2 session.`

   Le fichier `restjob.txt` créé contient des informations sur les périphériques d'origine et les emplacements initiaux des supports (lors de la sauvegarde de l'IDB) :
2. Modifiez le fichier `restjob.txt` pour indiquer le périphérique actuel ou l'emplacement dans lequel les supports se trouvent.
3. Exécutez la restauration avec la commande `omnioffl r -idb -read C:\TEMP\restjob.txt`.

Cette commande vous guide tout au long de la restauration de l'IDB et de la réexécution des fichiers de journal archivés après la dernière sauvegarde de l'IDB. Si vous ne disposez pas des fichiers journaux archivés, vous pouvez toujours mettre l'IDB à jour en important tous les supports utilisés depuis sa dernière sauvegarde.

Restauration de la base de données IDB sans le fichier de récupération de l'IDB

Utilisez cette procédure pour restaurer la base de données interne si le fichier de récupération de l'IDB n'est pas disponible.

Conditions préalables

- Montez un disque dont la taille est identique à celle du disque avant le sinistre sur les mêmes répertoires que lors de la sauvegarde de l'IDB (sur les systèmes Windows, les mêmes lettres de lecteur doivent être affectées). Si vous ne pouvez pas effectuer cette opération, suivez la procédure de récupération de l'IDB sur une configuration de disque/volume différente. Vous pouvez utiliser l'option `-preview` de la commande `omnioffl r` pour savoir où les fichiers seront restaurés.
- Dans la mesure du possible, déplacez le fichier `media.log` de l'installation précédente en lieu sûr. Celui-ci contient des informations sur les supports utilisés depuis la dernière sauvegarde de l'IDB. Il vous sera très utile pour mettre à jour l'IDB si les journaux de transactions ne sont pas disponibles.
- Installez Data Protector sur le Gestionnaire de cellule et sur le système auquel un périphérique est connecté (de préférence le périphérique utilisé pour la sauvegarde de l'IDB).
- Si l'IDB est installée sous HPE Serviceguard, les commandes suivantes doivent être exécutées sur le nœud actif avant la récupération automatique guidée :
  1. `cmhaltpkg` *`PackageName`*, où *`PackageName`* est le nom du package de cluster Data Protector. Cette commande arrête le package Data Protector et démonte le groupe de volumes Data Protector partagé.
  2. `vgchange -a e /dev/`*`vg_name`*, où *`vg_name`* est le nom du groupe de volumes partagés Data Protector. Cette commande permet d'activer le groupe de volumes Data Protector partagé. Pour afficher les liste des groupes de volumes du système, exécutez la commande `ll /dev/*/group`.
  3. `mount /dev/`*`vg_name/lv_name/MountPoint`*, où *`MountPoint`* est le nom du point de montage pour le groupe de volumes partagés Data Protector. Cette commande permet de monter le groupe de volumes Data Protector partagé.

  Lorsque la récupération automatique guidée est terminée, exécutez la commande `cmrunpkg` *`PackageName`* sur le nœud actif pour démarrer le package Data Protector.
- Si l'IDB est installée sur un serveur de clusters Symantec Veritas, mettez la ressource d'application Data Protectorhors ligne sur le nœud actif avant d'effectuer la récupération automatique guidée.

  Lorsque la récupération automatique guidée est terminée, mettez la ressource d'application Data Protectoren ligne sur le nœud actif pour démarrer le service Data Protector.
- Si l'IDB est installée sur un Microsoft Cluster Server, mettez les groupes de clusters `OBVS_HPDP_AS, OBVS_HPDP_IDB,` et `OBVS_HPDP_IDB_CP` hors ligne à l'aide de l'utilitaire d'administration des clusters et arrêtez le service `Inet` sur le nœud actif avant d'effectuer la récupération automatique guidée. Une fois la récupération automatique guidée terminée, mettez les groupes de clusters `OBVS_HPDP_AS, OBVS_HPDP_IDB, OBVS_HPDP_IDB_CP,` et `OBVS_MCRS` en ligne à l'aide de l'utilitaire de l'Administrateur de clusters, puis redémarrez le service `Inet`.

Procédure

1. Configurez le périphérique à l'aide de l'interface graphique de Data Protector.
2. Recherchez le support contenant la dernière sauvegarde de l'IDB.
3. Insérez le support dans le périphérique et utilisez la commande suivante pour afficher son contenu :

   `omnimlist -dev device_name`

   Les informations nécessaires à la restauration de l'IDB sont l'ID du support et celui de l'Agent de disque pour la session de sauvegarde à restaurer.
4. Utilisez la commande suivante pour afficher les informations concernant la configuration du périphérique :

   `omnidownload -dev device_name`

   Les informations nécessaires à la restauration de l'IDB sont les suivantes :

   - Mahost (hôte de l'Agent de support)
   - Politique (nombre) : Un numéro de politique peut être obtenu à l'aide de la traduction suivante : 1 pour les périphériques autonomes, 3 pour les périphériques chargeurs, 5 pour les bibliothèques de bandes magnéto-optiques, 6 pour les périphériques de contrôle externe, 8 pour la bibliothèque DAS GRAU, 9 pour la bibliothèque ACS StorageTek et 10 pour la bibliothèque SCSI.
   - Type de support (nombre) : Les numéros des types de supports sont définis dans la catégorie support dans le fichier `scsitab`. Pour l'emplacement exact, voir le sujet Prise en charge de nouveaux périphériques.
   - Adresse SCSI
   - Adresse SCSI du robot de bibliothèque (uniquement en cas d'utilisation de périphériques échangeurs de bibliothèque)
5. Exécutez la commande `omnioffl r` en utilisant les informations obtenues :

   `omnioffl r -idb -policy PolicyNumber -type MediaTypeNumber [-ioctl RoboticsSCSIAddress] -dev SCSIAddress -mahost MAClientName -maid MediumID -daid DiskAgentID`

   Par exemple, vous pouvez utiliser la commande suivante pour restaurer l'IDB depuis une session de sauvegarde avec l'ID de support `0100007f:3a486bd7:0410:0001` et l'ID d'Agent de disque `977824764`, avec un périphérique autonome de type DLT, connecté au système `company.dot.com` et l'adresse SCSI `scsi0:1:2:0` :

   ```
   omnioffl r -idb -policy 1 -type 10 -dev scsi0:1:2:0 -mahost company.dot.com -maid 0100007f:3a486bd7:0410:0001 -daid 977824764
   ```

Cette commande vous guide tout au long de la restauration de l'IDB et de la réexécution des fichiers de journal archivés depuis la dernière sauvegarde de l'IDB. Si vous ne disposez pas des fichiers de journal, vous pouvez toujours mettre l'IDB à jour en important tous les supports utilisés depuis sa dernière sauvegarde.

Restauration de la base de données IDB à partir d'une session spécifique de l'IDB

Utilisez cette procédure pour restaurer la base de données interne à partir d'une sauvegarde autre que la dernière si le fichier de récupération de l'IDB est disponible.

Conditions préalables

- Montez un disque dont la taille est identique à celle du disque avant le sinistre sur les mêmes répertoires que lors de la sauvegarde de l'IDB (sur les systèmes Windows, les mêmes lettres de lecteur doivent être affectées). Si vous ne pouvez pas effectuer cette opération, suivez la procédure de récupération de l'IDB sur une configuration de disque/volume différente. Vous pouvez utiliser l'option `-preview` de la commande `omnioffl r` pour savoir où les fichiers seront restaurés.
- Dans la mesure du possible, stockez le fichier `media.log` de l'installation précédente en lieu sûr. Celui-ci contient des informations sur les supports utilisés depuis la dernière sauvegarde de l'IDB. Il vous sera très utile pour mettre à jour l'IDB si les journaux de transactions ne sont pas disponibles.
- Installez Data Protector sur le Gestionnaire de cellule et sur le système auquel un périphérique est connecté (de préférence le périphérique utilisé pour la sauvegarde de l'IDB).
- Si l'IDB est installée sous HPE Serviceguard, les commandes suivantes doivent être exécutées sur le nœud actif avant la récupération automatique guidée :
  1. `cmhaltpkg` *`PackageName`*, où *`PackageName`* est le nom du package de cluster Data Protector. Cette commande arrête le package Data Protector et démonte le groupe de volumes Data Protector partagé.
  2. `vgchange -a e /dev/`*`vg_name`*, où *`vg_name`* est le nom du groupe de volumes partagés Data Protector. Cette commande permet d'activer le groupe de volumes Data Protector partagé. Pour afficher les liste des groupes de volumes du système, exécutez la commande `ll /dev/*/group`.
  3. `mount /dev/`*`vg_name/lv_name/MountPoint`*, où *`MountPoint`* est le nom du point de montage pour le groupe de volumes partagés Data Protector. Cette commande permet de monter le groupe de volumes Data Protector partagé.

  Lorsque la récupération automatique guidée est terminée, exécutez la commande `cmrunpkg` *`PackageName`* sur le nœud actif pour démarrer le package Data Protector.
- Si l'IDB est installée sur un serveur de clusters Symantec Veritas, mettez la ressource d'application HPE Data Protectorhors ligne sur le nœud actif avant d'effectuer la récupération automatique guidée.

  Lorsque la récupération automatique guidée est terminée, mettez la ressource d'application HPE Data Protectoren ligne sur le nœud actif pour démarrer le service HPE Data Protector.
- Si l'IDB est installée sur un Microsoft Cluster Server, mettez les groupes de clusters `OBVS_HPDP_AS, OBVS_HPDP_IDB,` et `OBVS_HPDP_IDB_CP` hors ligne à l'aide de l'utilitaire d'administration des clusters et arrêtez le service `Inet` sur le nœud actif avant d'effectuer la récupération automatique guidée. Une fois la récupération automatique guidée terminée, mettez les groupes de clusters `OBVS_HPDP_AS, OBVS_HPDP_IDB, OBVS_HPDP_IDB_CP,` et `OBVS_MCRS` en ligne à l'aide de l'utilitaire de l'Administrateur de clusters, puis redémarrez le service `Inet` et exécutez la commande `omnidbutil -fixmpos`.

Procédure

1. Vérifiez toutes les sauvegardes avec la commande suivante :

   ```
   omniofflr -idb -autorecover -logview -skiprestore
   ```

2. Choisissez la session de sauvegarde à restaurer, puis effectuez la restauration de l'IDB en exécutant la commande suivante :

   ```
   omniofflr -idb -autorecover -session SessionID
   ```

Cette commande vous guide tout au long de la restauration de l'IDB et de la réexécution des fichiers de journal archivés depuis la dernière sauvegarde de l'IDB. Si vous ne disposez pas des fichiers journaux archivés, vous pouvez toujours mettre l'IDB à jour en important tous les supports utilisés depuis sa dernière sauvegarde.

Restauration de la base de données IDB sur un hôte Gestionnaire de cellule différent

Utilisez cette procédure pour la récupération de la base de données IDB sur un hôte Gestionnaire de cellule différent.

1. Installez Data Protector sur un nouvel hôte Gestionnaire de cellule et importez le périphérique contenant la sauvegarde IDB de l'ancien hôte Gestionnaire de cellule.
2. Restaurez uniquement les fichiers de configuration vers un nouvel emplacement. Par exemple, `/tmp/idb/config`.
3. Effectuez une copie du fichier d'origine `/etc/opt/omni/server/cell/cell_info`.
4. Restaurez la base de données IDB complète vers un nouvel emplacement. Par exemple, `/tmp/idb/newidb`.
   - Pour restaurer des fichiers de base de données, sélectionnez les options **StartDatabaseServer** et **UseRestoredDatabaseAsNewDatabase**.
   - Pour les fichiers binaires de catalogue en tant que destination, sélectionnez Restaurer vers l'emplacement d'origine.
   - Pour les fichiers de configuration en tant que destination, sélectionnez **Restaurer vers l'emplacement d'origine** puis sélectionnez la résolution de conflit **Ecraser**.
5. Une fois la restauration terminée sans erreurs, créez une copie des fichiers originaux suivants (en tant que mesure de précaution) :
   - `/etc/opt/omni/server/AppServer/standalone.xml`
   - `/etc/opt/omni/server/idb/idb.config`
   - `/etc/opt/omni/server/idb/ulist`
6. Arrêtez les services Data Protector en exécutant la commande suivante : `/opt/omni/sbin/omnisv stop`
7. Ecrasez le fichier suivant : `/etc/opt/omni/server/cell/cell_info` par une copie du fichier effectuée à l'étape 3.

8. Ouvrez le fichier `/etc/opt/omni/server/AppServer/standalone.xml` dans l'éditeur de votre choix, puis recherchez `keystore-password` et `truststore-password` et prenez-en note. Ils sont généralement identiques.
9. Ouvrez le fichier `/etc/opt/omni/client/components/webservice.properties` dans l'éditeur de votre choix, remplacez `keystore-password` et `truststore-password` par les valeurs issues du fichier `standalone.xml`, enregistrez les modifications et fermez le fichier.

   REMARQUE : Dans un environnement de cluster, vous devez éditer le fichier webservice.properties sur tous les nœuds du cluster.
10. Regénérez le certificat en exécutant la commande suivante : `/opt/omni/bin/perl /opt/omni/sbin/omnigencert.pl -server_id <hostname> -user_id hpdp -store_password <your keystore password>`
11. Assurez-vous que les fichiers suivants ne contiennent pas le nom d'hôte de l'ancien Gestionnaire de cellule :
    - `/etc/opt/omni/client/components/dp-jobexecutionengine-backup\webservice.properties /etc/opt/omni/client/components/dp-jobexecutionengine-consolidation\webservice.properties`
    - `/etc/opt/omni/client/components/dp-jobexecutionengine-copy\webservice.properties`
    - `/etc/opt/omni/client/components/dp-jobexecutionengine-verification\webservice.properties`
    - `/etc/opt/omni/client/components/dp-loginprovider\webservice.properties`
    - `/etc/opt/omni/client/components/dp-Scheduler-gui\webservice.properties`
    - `/etc/opt/omni/client/components/dp-webservice-server\webservice.properties`
    - `/etc/opt/omni/client/components/jce-dispatcher\webservice.properties`
    - `/etc/opt/omni/client/components/jce-serviceregistry\webservice.properties`
    - `/etc/opt/omni/client/components/webservice.properties`
12. Ajoutez la variable suivante au fichier omnirc - `/opt/omni/.omnirc: OB2_CERT_VERIFYHOST=0`. Si le fichier omnirc n'existe pas, créez un fichier texte vide et renommez-le `.omnirc` ou renommez `.omnirc.TMPL .omnirc`
13. Démarrez les services Data Protector en exécutant la commande suivante : `/opt/omni/sbin/omnisv start`
14. Exécutez la commande suivante pour changer l'appartenance de certains fichiers Data Protector : `/opt/omni/sbin/omnidbutil -change_cell_name <old_cm_hostname>`
15. Exécutez la commande suivante pour supprimer les sessions en cours : `/opt/omni/sbin/omnidbutil -clear`
16. Dans le client de l'interface utilisateur graphique Windows, supprimez le dossier contenant l'ancien certificat. Une fois que vous avez démarré les services Data Protector, l'interface utilisateur graphique Data Protector importe un nouveau certificat depuis Gestionnaire de cellule.

L'ancien certificat se trouve dans le chemin d'accès suivant :
`C:\Users\<USERNAME>\AppData\Local\Hewlett-Packard\Data Protector\ca\<NEW_CM_HOSTNAME>"`

17. Suivez les étapes suivantes facultatives :
    a. Exécutez la commande suivante pour confirmer que IDB utilise des fichiers via un nouvel emplacement (les fichiers d'espace de table et les journaux à écriture anticipée se trouvent à un nouvel emplacement tandis que les DCBF se trouvent dans le dossier d'origine) : `/opt/omni/sbin/omnidbutil -show_db_files`
    b. Mettez à jour les fichiers contenant le nom d'hôte de l'ancien Gestionnaire de cellule (généralement dans la liste d'utilisateurs, les barlists et les fichiers de configuration). Vous les trouverez en exécutant la commande suivante : `grep -rnw /etc/opt/omni -e <OLD_CM_HOSTNAME>`
    c. Reconfigurez les périphériques pour utiliser le nouveau Gestionnaire de cellule.

Mise à jour de l'IDB par l'importation de supports

Si vous ne disposez pas des fichiers journaux archivés, mettez l'IDB à jour en important tous les supports utilisés depuis sa dernière sauvegarde. Faites cela une fois la restauration de l'IDB terminée.

Procédure

1. Démarrez les processus et services Data Protector.
2. Augmentez le compteur de sessions. Lorsque vous avez initialisé et restauré l'IDB, le compteur était défini sur `0`. Ainsi, les nouvelles sessions auront le même ID de session que celle déjà démarrée ce jour-là.

   La commande suivante définit le décompte de sessions sur `200`, ce qui est suffisant dans la plupart des cas :

   ```
   omnidbutil -set_session_counter 200
   ```

   Si nécessaire, vous pouvez maintenant commencer les sauvegardes.
3. Exportez et importez les supports avec la dernière sauvegarde de l'IDB. Cela crée des informations cohérentes sur la dernière sauvegarde de l'IDB.
4. Importez (exportez si déjà présents dans l'IDB) les supports utilisés entre la dernière sauvegarde de l'IDB et la récupération de l'IDB. Pour une liste des supports utilisés, consultez le fichier `media.log` se trouvant à l'emplacement des fichiers Data Protectorjournaux par défaut du serveur .
5. Exécutez la commande `omnidbcheck`.

L'IDB complète devrait être récupérée correctement.

> **REMARQUE :**
> Si vous récupérez une IDB qui comprend une CMMDB ou MMDB distante vers une disposition de disques différente, exécutez la commande `omnidbutil -cdbsync` après la mise à jour de l'IDB.

Chapitre 5: Environnement Manager-of-Managers

A propos de l'environnement MoM

Le concept de Data ProtectorManager-of-Managers permet aux administrateurs de gérer de façon centralisée et à partir d'un point unique un environnement étendu, également nommé environnement de sauvegarde d'entreprise avec plusieurs cellules Data Protector à partir d'un point unique (gestion centralisée).

Il est ainsi possible de gérer une croissance quasiment illimitée de l'environnement de sauvegarde : vous pouvez ajouter de nouvelles cellules ou diviser des cellules existantes.

Notez que chaque client MoM et le Gestionnaire MoM doivent utiliser la même version de Data Protector.

Le Manager-of-Managers présente les caractéristiques suivantes :

- Gestion centralisée de toutes les tâches

  Data Protector permet la configuration, la gestion et le contrôle de l'environnement de sauvegarde d'entreprise à partir du point unique. Cela comprend la configuration des sauvegardes et restaurations, la gestion des supports, la surveillance et la génération de rapports sur l'état de l'ensemble de l'environnement de sauvegarde.
- Base de données centralisée de gestion des supports (CMMDB)

  Toutes les cellules de l'environnement peuvent facultativement partager une base de données commune, centrale pour la gestion des supports et des périphériques de l'entreprise. La CMMDB permet de partager des supports et des périphériques haut de gamme entre plusieurs cellules dans un environnement MoM. Les périphériques d'une cellule donnée (qui utilise la CMMDB) sont ainsi accessibles aux autres cellules qui utilisent la CMMDB.
- Gestion centralisée des licences

  Data Protector vous permet de configurer la gestion centralisée des licences pour l'environnement MoM tout entier. Toutes les licences Data Protector sont installées et conservées sur le Gestionnaire MoM. En fonction de vos besoins, vous pouvez affecter des licences à des cellules spécifiques.

A propos de la base de données CMMDB

Dans un grand environnement multicellules comportant des périphériques de sauvegarde, haut de gamme, il peut être judicieux de partager les périphériques et les supports entre plusieurs cellules. Vous pouvez effectuer cela avec une seule CMMDB (base de données centralisée de gestion des supports) pour toutes les cellules et en conservant une CDB (base de données catalogue) particulière à chaque cellule. Vous pouvez ainsi partager des supports et des périphériques tout en conservant les fonctions de sécurité de la structure multicellules.

Partage des supports

Avec la CMMDB, les supports ne peuvent appartenir qu'à la cellule Data Protector qui a effectué sur eux la première sauvegarde. Le nom du propriétaire du support apparaît dans l'affichage des supports. Tant qu'un support est protégé, il est possible d'y ajouter uniquement les sauvegardes effectuées à partir de cette cellule. Chaque support contenant des données protégées possède des informations indiquant la cellule qui détient actuellement les données. Lorsque la protection arrive à expiration, le support est à nouveau disponible pour une autre cellule.

Initialisation des supports

Si une bande a été initialisée par une cellule, il est possible de l'utiliser avec toute autre cellule tant qu'elle ne contient pas de données protégées. Si une bande est chargée dans une bibliothèque sans avoir été initialisée, il est possible de l'initialiser à partir de n'importe quelle cellule à condition qu'une stratégie souple ait été définie et qu'aucune autre bande ne soit disponible. Les règles d'allocation de supports s'appliquent exactement de la même manière aux bandes partagées, mais les supports avec ajout possible ne peuvent recevoir d'ajout que de la cellule qui en est propriétaire.

IMPORTANT :
Prenez en compte ce qui suit :

- La MMDB centralisée a des incidences considérables sur l'attribution des licences. Immédiatement après le changement de la MMDB de locale à distante, toutes les licences associées à des bibliothèques et des périphériques sont reprises (validées) au MoM et doivent être supprimées des cellules client.
- Une cellule de l'environnement d'entreprise doit avoir accès à la CMMDB pour permettre l'exécution d'une sauvegarde. Par exemple, ceci est le cas si une panne réseau survient entre la cellule et celle MoM. Une connexion réseau fiable entre la cellule MoM et les autres cellules de Data Protector est nécessaire.

Procédure de configuration de l'environnement MoM

Conditions préalables

- Vous devez choisir un système pour le MoM Manager. Il doit s'agir d'un système très fiable : un Gestionnaire de cellule Data Protector sur lequel le logiciel est installé.
- Installez les licences requises sur la cellule MoM et sur chaque future cellule de client MoM.

Procédure de configuration de l'environnement MoM

La procédure de configuration de l'environnement MoM se déroule en plusieurs étapes. Pour cela, vous devez :

1. Installer le Gestionnaire MoM.
2. Importer les cellules Data Protector dans l'environnement MoM.

3. Créer un utilisateur Data Protector dans le groupe d'utilisateurs `admin` sur chaque cellule de l'environnement MoM qui agira en tant qu'administrateur MoM.
4. Redémarrer les services Data Protector.

Si vous le souhaitez, vous pouvez également configurer une base de données centralisée de gestion des supports, et une gestion centralisée des licences, et distribuer la configuration du MoM.

Installation du Gestionnaire MoM

Pour installer un environnement d'entreprise, configurez l'un des Gestionnaires de cellule en tant que Gestionnaire MoM.

Procédure

1. Dans la liste de contexte, cliquez sur **Clients**.
2. Dans le menu Actions, cliquez sur **Configurer CM comme serveur Manager-of-Managers Data Protector.**
3. Redémarrez les services Data Protector.
4. Lancez l'interface utilisateur MoM en sélectionnant **Data ProtectorManager-of-Managers** dans le groupe de programmes Data Protector.

   Vous pouvez également exécuter la commande `mom` depuis le répertoire *`répertoire_Data_Protector`*`\bin`\bin. Pour plus d'informations sur la commande`mom`, reportez-vous à la page de manuel `omnigui` ou à la *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Ajout d'un administrateur MoM à des cellules

Un administrateur MoM peut effectuer des tâches d'administration dans toutes les cellules de l'environnement d'entreprise.

Conditions préalables

Vous devez avoir un utilisateur appartenant au groupe d'utilisateurs `admin` dans chaque Gestionnaire de cellule de l'environnement MoM. Par exemple, vous pouvez avoir un utilisateur appelé `MoM_Admin`. Cet utilisateur sera l'administrateur MoM.

Procédure

1. Utilisez le Gestionnaire Data Protector pour vous connecter à chaque Gestionnaire de cellule de l'environnement MoM en tant que membre du groupe d'utilisateurs `admin` (le droit utilisateur `User configuration` est nécessaire).
2. Ajoutez l'utilisateur désigné comme administrateur MoM au groupe d'utilisateurs Data Protector `admin`.

Importation de cellules

L'importation d'une cellule dans un environnement MoM permet de gérer celle-ci de manière centralisée avec le Gestionnaire MoM.

Les clients cluster s'identifient auprès du Gestionnaire MoM avec leurs noms de serveur virtuel. Si vous importez un cluster dans un environnement MoM, utilisez uniquement son nom de serveur virtuel.

Conditions préalables

- L'utilisateur actif doit être membre du groupe d'utilisateurs `Admin` sur le Gestionnaire de cellule de la cellule à importer.

Procédure

1. Dans le Manager-of-Managers Data Protector, cliquez sur **Clients** dans le menu contextuel.
2. Cliquez avec le bouton droit sur **Clients d'entreprise**, puis cliquez sur **Importer Gestionnaire de cellule**.
3. Sélectionnez le Gestionnaire de cellule à importer et cliquez sur **Terminer**.

Redémarrage des services HPE Data Protector dans l'environnement MoM

Après la configuration de l'environnement MoM, vous êtes invité à redémarrer les services Data Protector.

Si vous utilisez le `Windows Service Control Manager` pour arrêter et démarrer les services sur le Gestionnaire de cellule, seules les copies actuelle et précédente du journal de la base de données sont conservées. L'utilisation de la commande `omnisv` permet d'enregistrer tous les journaux précédents de la base de données.

Arrêt des services Data Protector

Gestionnaire de cellule dans un environnement sans cluster

Exécutez la commande suivante : `omnisv -stop.`

Gestionnaire de cellule sur HPE Serviceguard

Exécutez la commande suivante : `cmhaltpkg` *`PackageName`*, où *`PackageName`* est le nom du package de cluster Data Protector.

Cette commande arrête le package Data Protector et démonte le groupe de volumes Data Protector partagé.

Gestionnaire de cellule sur Symantec Veritas Cluster Server

Mettez la ressource d'application HPE Data Protector hors ligne.

Gestionnaire de cellule sur Microsoft Cluster Server

Mettez les groupes de clusters `OBVS_HPDP_AS`, `OBVS_HPDP_IDB`, et `OBVS_HPDP_IDB_CP` hors ligne (à l'aide de l'utilitaire `Cluster Administrator` sur le nœud actif).

Démarrage des services Data Protector

Gestionnaire de cellule dans un environnement sans cluster

Exécutez la commande suivante : `omnisv -start`

Gestionnaire de cellule sur HPE Serviceguard

Redémarrez le package Data Protector à l'aide de la commande `cmrunpkg -n` *`NodeName PackageName`*.

Gestionnaire de cellule sur Symantec Veritas Cluster Server

Mettez la ressource d'application HPE Data Protector en ligne.

Gestionnaire de cellule sur Microsoft Cluster Server

Mettez les groupes de cluster `OBVS_HPDP_AS`, `OBVS_HPDP_IDB`, `OBVS_HPDP_IDB_CP`, and `OBVS_MCRS` en ligne en utilisant l'utilitaire `Cluster Administrator`.

Configuration de la base de données CMMDB

Configurez la base de données CMMDB pour bénéficier d'une gestion centralisée des supports. Si vous ne configurez pas de base de données CMMDB, chaque cellule aura sa propre IDB.

Lors de la configuration, une base de données de gestion des supports locale est fusionnée avec la base de données CMMDB, si vous le choisissez. Vous pouvez décider si chaque cellule utilisera la base de données CMMDB ou sa propre base de données MMDB locale.

> **IMPORTANT :**
> Une fois que la base de données CMMDB est configurée et que vous avez commencé à l'utiliser, vous ne pouvez plus la diviser en bases de données MMDB locales. N'essayez pas de rétablir l'ancien état d'une base de données MMDB. Créez-en plutôt une nouvelle.

A prendre en compte

Si vous configurez une nouvelle cellule (et que les périphériques et les supports ne sont pas encore configurés), il est inutile de fusionner la base de données. Seules les cellules avec des périphériques et

des supports configurés doivent être fusionnées avec la base de données CMMDB.

Conditions préalables

- Vérifiez que les Gestionnaires de cellule Data Protector dans toutes les cellules disposent de la même version de Data Protector installée et en cours d'exécution.
- Vérifiez qu'aucune session de sauvegarde, de restauration ou de gestion des supports n'est en cours dans les cellules à ajouter à la base de données CMMDB.

Configuration de la base de données CMMDB sur une cellule client

Procédure

1. Connectez-vous au responsable de Cellule de la cellule client en tant que membre du groupe utilisateur `admin`.
2. Créez le fichier contenant le nom du serveur MMDB (entier). Sur les systèmes Windows, enregistrez le fichier au format Unicode :

   Systèmes Windows : *données_programme_Data_Protector*`\Config\server\cell\mmdb_server`

   Systèmes UNIX : `/etc/opt/omni/server/cell/mmdb_server`
3. Permet à MoM Manager d'établir la connexion à une cellule en modifiant le fichier `pg_hba.conf`, situé dans le répertoire `pg` de l'emplacement de la Base de Données Interne.

   Ouvrez le fichier dans un éditeur de texte et ajoutez la ligne suivante :

   `host hpdpidb hpdpidb_app` *MoM_Server_IP_Address*`/32 trust`

   après les lignes suivantes

   ```
   # IPv4 local connections:
   host all all 127.0.0.1/32 md5
   ```

   Enregistrez le fichier.

   > **REMARQUE :**
   > Si le Responsable de Cellule sur un client MoM fait partie d'un environnement de clusters, vous devez indiquer soit l'adresse IP de tous les noeuds de cluster (une ligne par noeud), soit le sous-réseau du cluster dans le fichier `pg_hba.conf` sur le Responsable de Cellule du client MoM.

   Ouvrez le fichier dans un éditeur de texte et ajoutez la ligne suivante :

   `host hpdpidb hpdpidb_app` *Cluster_Subnet* `trust`

   après les lignes suivantes

   ```
   # IPv4 local connections:
   host all all 127.0.0.1/32 md5
   ```

   Enregistrez le fichier.
4. Redémarrez les services Data Protector.
5. Mettez à jour les fichiers de configuration en exécutant la commande suivante :

   ```
   omnicc -update_mom_server
   ```

Répétez les étapes pour toutes les cellules client pour lesquelles vous voulez fusionner la base de données MMDB avec la base de données CMMDB.

Configuration de la base de données CMMDB sur le Gestionnaire MoM

Procédure

1. Connectez-vous au Responsable-des-Responsables et copiez le répertoire d'espaces de tableau `idb` vers un emplacement provisoire pour des raisons de sécurité.

   Le `idb` est un sous-répertoire à l'emplacement de la Base de Données Interne.
2. Exécutez la commande suivante pour fusionner la base de données MMDB locale avec la base de données CMMDB :

   `omnidbutil -mergemmdb` *`MoM_Client_Cell_Manager_Hostname`*

   Vérifiez que le port 7112 du service (hpdp-idb) de la base de données interne est ouvert sur le Gestionnaire MoM et sur le Gestionnaire de cellule client lors de l'exécution de la commande. Vous pouvez fermer les ports une fois la fusion exécutée.
3. Exécutez la commande suivante pour synchroniser la base de données catalogue locale :

   `omnidbutil -cdbsync` *`MoM_Client_Cell_Manager_Hostname`*
4. Modifiez les noms dupliqués des périphériques et des pools de supports. Cette duplication se produit toujours sur les pools par défaut, s'ils existent sur les deux cellules. Les noms dupliqués ont un "`_N`" attaché à leur nom, lorsque `N` représente un chiffre. Dans ce cas, modifiez manuellement les spécifications de sauvegarde qui utilisent ces périphériques afin d'utiliser les nouveaux noms de périphériques.

Répétez les étapes pour toutes les cellules client pour lesquelles vous voulez fusionner la base de données MMDB avec la base de données CMMDB.

A propos de la gestion centralisée des licences

La gestion centralisée des licences signifie que toutes les licences sont configurées sur le Gestionnaire MoM et qu'elles peuvent être allouées à des cellules spécifiques selon les besoins. Cette fonction permet de simplifier la gestion des licences. L'administrateur MoM est chargé de l'administration des licences, y compris leur distribution et leur déplacement, pour toutes les cellules de l'environnement MoM.

L'installation de la gestion centralisée des licences est facultative. A la place, il est possible d'installer des licences individuelles sur chaque Gestionnaire de cellule. Ces licences sont restreintes à la cellule sur laquelle elles sont installées et leur administration doit s'effectuer en local.

Installation de la gestion centralisée des licences

Installez la gestion centralisée des licences pour simplifier la gestion des licences dans les environnements d'entreprise.

Conditions préalables

Si vous consolidez des cellules Data Protector existantes dans un environnement MoM, envoyez une demande au Centre de remise des mots de passe *HPE* pour déplacer les licences des Gestionnaires de cellule existants vers le nouveau Gestionnaire MoM.

Procédure

1. Connectez-vous au Gestionnaire MoM et créez le fichier `licdistrib.dat` :

   Systèmes Windows : *données_programme_Data_Protector*`\Config\server\cell\licdistrib.dat`

   Systèmes UNIX : `/etc/opt/omni/server/cell/licdistrib.dat`
2. Connectez-vous à chaque Gestionnaire de cellule dans l'environnement MoM et créez le fichier `lic_server` avec le nom du Gestionnaire MoM :

   Systèmes Windows : *données_programme_Data_Protector*`\Config\server\cell\lic_server`

   Systèmes UNIX : `/etc/opt/omni/server/cell/lic_server`
3. Arrêtez et redémarrez les services Data Protector sur chaque Gestionnaire de cellule où les modifications ont été effectuées.
4. Dans le Manager-of-Managers Data Protector, cliquez sur **Clients** dans le menu contextuel.
5. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le Gestionnaire de cellule contenant les informations de gestion des licences à modifier, puis cliquez sur **Configurer l'attribution des licences** pour ouvrir l'assistant. Les types et les nombres de licences disponibles pour le Gestionnaire de cellule sélectionné s'affichent.

   > **REMARQUE :**
   > Identifiez un client cluster avec son nom d'hôte virtuel.
6. Cliquez sur l'option **Distant** pour modifier la gestion des licences du paramètre local sur le paramètre distant. La colonne Utilisé est remplacée par la colonne Alloué.
7. Modifiez la configuration de la licence. Seule la colonne Alloué est accessible lors de la modification.
   - Pour libérer (abandonner) un type de licence, ce qui augmente le nombre de licences disponibles, réduisez le nombre correspondant dans la colonne Alloué.
   - Pour attribuer un type de licence, augmentez son nombre correspondant dans la colonne Alloué.
8. Cliquez sur **Terminer** pour appliquer la configuration.
9. Répétez les étapes pour tous les Gestionnaires de cellule pour lesquels vous souhaitez configurer la gestion centralisée des licences.
10. Arrêtez et redémarrez les processus Data Protector à l'aide des commandes `omnisv -stop` et `omnisv -start`.

    Si le Gestionnaire de cellule est configuré sur HPE Serviceguard, exécutez la commande `cmhaltpkg` *`PackageName`* pour arrêter et la commande `cmrunpkg -n` *`NodeName PackageName`*

pour démarrer le package Data Protector, où *PackageName* est le nom du package de cluster Data Protector.

Si le Gestionnaire de cellule est configuré sur Symantec Veritas Cluster Server, mettez la ressource d'application Data Protector hors ligne puis remettez la ressource d'application Data Protector en ligne.

Les modifications prennent effet lorsque vous arrêtez et redémarrez les services Data Protector sur chaque Gestionnaire de cellule où les modifications ont été effectuées.

> **REMARQUE :**
> Data Protector vérifie la configuration de la licence avec le Gestionnaire MoM toutes les heures. En cas de problème de communication ou si le Gestionnaire MoM est indisponible, l'état de la gestion des licences est conservé pendant 72 heures. Si les problèmes ne sont pas résolus dans un délai de 72 heures, les licences locales sont utilisées.

Désactivation de la gestion centralisée des licences

Il est possible de désactiver la gestion centralisée des licences et de la convertir en une gestion locale des licences.

Procédure

1. Dans le Manager-of-Managers Data Protector, cliquez sur **Clients** dans le menu contextuel.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le Gestionnaire de cellule pour lequel vous souhaitez désactiver la gestion centralisée des licences, puis cliquez sur **Configurer l'attribution de licences** pour ouvrir l'assistant. Les types et les nombres de licences disponibles pour le Gestionnaire de cellule sélectionné s'affichent.

   > **REMARQUE :**
   > Identifiez un client cluster avec son nom d'hôte virtuel.

3. Cliquez sur l'option **Local** pour modifier la gestion des licences du paramètre distant sur le paramètre local.
4. Cliquez sur **Terminer** pour appliquer la configuration.
5. Répétez les étapes pour les Gestionnaires de cellule pour lesquels vous souhaitez désactiver la gestion centralisée des licences.
6. Connectez-vous au Gestionnaire MoM et montez le répertoire `cell` qui réside dans le répertoire de configuration du serveur Data Protector par défaut.
7. Renommez le fichier `licdistrib.dat`, par exemple en `licdistrib.old`.

Les modifications prennent effet lorsque vous arrêtez et redémarrez les services Data Protector à l'aide des commandes `omnisv -stop` et `omnisv -start` dans le Gestionnaire MoM et dans chaque Gestionnaire de cellule où les modifications ont été effectuées.

Si le Gestionnaire de cellule est configuré sur HPE Serviceguard, exécutez la commande `cmhaltpkg` *PackageName* pour arrêter et la commande `cmrunpkg -n` *NodeName PackageName* pour démarrer le package Data Protector, où *PackageName* est le nom du package de cluster Data Protector.

Si le Gestionnaire de cellule est configuré sur Symantec Veritas Cluster Server, mettez la ressource d'application HPE Data Protector hors ligne puis remettez la ressource d'application HPE Data Protector en ligne.

A propos de l'administration de l'environnement MoM

Le MoM permet à l'utilisateur de configurer, gérer et contrôler un environnement de sauvegarde d'entreprise à partir d'un point central.

Depuis l'interface utilisateur du MoM, vous pouvez importer et exporter des cellules, déplacer des clients entre des cellules et distribuer la configuration du MoM à d'autres cellules de l'environnement.

Vous pouvez effectuer d'autres tâches sur le Gestionnaire MoM, comme si vous étiez un administrateur local. Suivez la procédure standard pour configurer une sauvegarde et une restauration, gérer des périphériques et des supports pour une cellule spécifique, configurer des utilisateurs et groupes d'utilisateurs Data Protector, ajouter des clients, surveiller des sessions en cours et l'état de l'environnement de sauvegarde et pour configurer des rapports et des notifications.

> **REMARQUE :**
> Vous pouvez configurer les périphériques connectés à des clients dans des cellules individuelles uniquement à partir des Gestionnaires de cellule respectifs, et non à partir du Gestionnaire MoM. Seuls les périphériques connectés directement à des Gestionnaires de cellule peuvent être configurés à partir du Gestionnaire MoM.

Exportation de cellules

L'exportation d'une cellule supprime celle-ci de l'environnement MoM.

Les clients cluster s'identifient auprès du Gestionnaire MoM avec leurs noms de serveur virtuel. Si vous exportez un cluster dans un environnement MoM, utilisez uniquement son nom de serveur virtuel.

Procédure

1. Dans le Manager-of-Managers Data Protector, cliquez sur **Clients** dans le menu contextuel.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le Gestionnaire de cellule à exporter, puis cliquez sur **Exporter Gestionnaire de cellule**.
3. Confirmez ensuite votre choix.

Déplacement de systèmes client entre des cellules

Data Protector vous permet de déplacer des systèmes entre des cellules. Au cours de ce processus, Data Protector effectue les opérations suivantes :

- Il vérifie que le client à déplacer est configuré dans une spécification de sauvegarde et supprime tous les objets sauvegarde appartenant à ce client des spécifications de sauvegarde configurées sur le Gestionnaire de cellule d'origine, tandis que les objets sauvegarde des autres clients restent intacts. Data Protector vérifie ensuite que les spécifications de sauvegarde ne contiennent aucun objet sauvegarde orphelin après le déplacement du client sur une autre cellule.

- Il vérifie s'il y a des périphériques configurés sur le système et vous guide tout au long de la procédure de déplacement des périphériques vers un autre système.
- Il vérifie si des supports sont utilisés dans les périphériques de ce système et vous guide tout au long de la procédure de déplacement des supports.

Procédure

1. Dans le Manager-of-Managers Data Protector, cliquez sur **Clients** dans le menu contextuel.
2. Développez le Gestionnaire de cellule où se trouve le système client à déplacer vers une autre cellule.
3. Cliquez avec le bouton droit sur ce système client, puis cliquez sur **Déplacer système client vers autre cellule** pour ouvrir l'assistant.
4. Sélectionnez le Gestionnaire de cellule cible.
5. Cliquez sur **Terminer** pour déplacer le client.

Désactivation de la gestion centralisée des licences

Data Protector vous permet de créer une spécification de classe d'utilisateur commune, des paramètres de fichier Jours chômés, option globale et de mise au coffre dans tous les Gestionnaires de cellule dans un environnement MoM.

Conditions préalables

Créez sur le Gestionnaire MoM la spécification de classe d'utilisateur, les paramètres de fichier de jours chômés et les paramètres d'options globales souhaités.

Procédure

1. Dans le Manager-of-Managers Data Protector, cliquez sur **Clients** dans le menu contextuel.
2. Cliquez avec le bouton droit sur **Clients d'entreprise**, puis cliquez sur **Distribuer Configuration**.
3. Dans la boîte de dialogue correspondante, sélectionnez le type de configuration et les Gestionnaires de cellule auxquels vous souhaitez distribuer la configuration sélectionnée.
4. Cliquez sur **Terminer** pour distribuer la configuration.

Configuration d'utilisateurs HPE Data Protector

Vous ajoutez des utilisateurs ou des groupes d'utilisateurs à un environnement MoM comme vous le feriez pour un Gestionnaire de cellule unique. Cette procédure entraîne la mise à jour de tous les Gestionnaires de cellule avec les nouveaux utilisateurs.

Procédure

1. Dans le Manager-of-Managers Data Protector, cliquez sur **Utilisateurs** dans le menu contextuel.
2. Sélectionnez le Gestionnaire de cellule auquel vous souhaitez ajouter des utilisateurs.

3. Dans le menu Edition, cliquez sur **Ajouter** et sélectionnez **Utilisateurs** pour ajouter un utilisateur, ou **Groupe d'utilisateurs** pour ajouter un groupe d'utilisateurs.
4. Saisissez les informations requises et cliquez sur **Terminer**.

Ajout d'un utilisateur à d'autres cellules

Vous pouvez ajouter des utilisateurs existants à d'autres cellules dans l'environnement MoM. L'utilisateur est automatiquement ajouté au même groupe d'utilisateurs dans le Gestionnaire de cellule cible que dans le Gestionnaire de cellule source.

> **REMARQUE :**
> Si le groupe auquel l'utilisateur appartient sur le Gestionnaire de cellule source n'existe pas dans le Gestionnaire de cellule cible, l'utilisateur ne peut pas être ajouté à la cellule.

Procédure

1. Dans le Manager-of-Managers Data Protector, cliquez sur **Utilisateurs** dans le menu contextuel.
2. Dans la fenêtre de navigation, développez le Gestionnaire de cellule, puis le groupe d'utilisateur dans lequel se trouve l'utilisateur.
3. Cliquez avec le bouton droit sur l'utilisateur, puis sur **Ajouter utilisateur à d'autres cellules** pour ouvrir l'assistant.
4. Sélectionnez le(s) Gestionnaire(s) de cellule cible(s).
5. Cliquez sur **Terminer** pour quitter l'assistant.

Suppression d'un utilisateur de certaines cellules

Vous pouvez supprimer des utilisateurs des cellules dans l'environnement MoM.

Procédure

1. Dans le Manager-of-Managers Data Protector, cliquez sur **Utilisateurs** dans le menu contextuel.
2. Dans la fenêtre de navigation, développez le Gestionnaire de cellule, puis le groupe d'utilisateur dans lequel se trouve l'utilisateur.
3. Cliquez avec le bouton droit sur l'utilisateur, puis sur **Supprimer utilisateur de certaines cellules** pour ouvrir l'assistant.
4. Sélectionnez le(s) Gestionnaire(s) de cellule du ou desquels vous voulez supprimer l'utilisateur.
5. Cliquez sur **Terminer** pour quitter l'assistant.

Gestion des périphériques et supports d'une cellule spécifique

Vous pouvez configurer des périphériques et des supports pour toute cellule de votre environnement d'entreprise.

Procédure

1. Dans le Manager-of-Managers Data Protector, cliquez sur **Clients** dans le menu contextuel.
2. Sélectionnez la cellule dont vous souhaitez gérer les périphériques et les supports.
3. Dans le menu **Outils**, cliquez sur **Administration périphériques et supports**.
   Un Gestionnaire Data Protector s'ouvre en affichant le contexte Périphériques et supports.
4. Configurez les périphériques et les supports comme si vous étiez un administrateur local.

> **REMARQUE :**
> Vous pouvez configurer les périphériques connectés à des clients dans des cellules individuelles uniquement à partir des Gestionnaires de cellule respectifs, et non à partir du Gestionnaire MoM. Seuls les périphériques connectés directement à des Gestionnaires de cellule peuvent être configurés à partir du Gestionnaire MoM.

Gestion de la base de données interne d'une cellule spécifique

Vous pouvez gérer la base de données interne pour toute cellule de votre environnement d'entreprise.

Procédure

1. Dans le Manager-of-Managers Data Protector, cliquez sur **Clients** dans le menu contextuel.
2. Sélectionnez le Gestionnaire de cellule à gérer.
3. Dans le menu **Outils**, cliquez sur **Administration base de données**. Dans le contexte de la base de données interne, effectuez les tâches d'administration de la base comme si vous étiez un administrateur local.

Chapitre 6: Gestion de clusters

A propos de la gestion de clusters

Pour plus d'informations sur les concepts de gestion de clusters, l'architecture et HPE Data Protector dans un environnement de cluster, consultez le *Guide conceptuel HPE Data Protector*.

Pour plus d'informations sur l'installation de HPE Data Protector dans un environnement de cluster, consultez le *Guide d'installation HPE Data Protector*.

À propos de l'intégration de HPE Data Protector avec Microsoft Cluster Server

Pour plus d'informations sur les concepts de gestion de clusters, l'architecture et HPE Data Protector dans un environnement de cluster, consultez le *Guide conceptuel HPE Data Protector*.

Pour plus d'informations sur l'installation de HPE Data Protector dans un environnement de cluster, consultez le *Guide d'installation HPE Data Protector*.

Entre autres fonctions de haute disponibilité, Data Protector fournit une intégration avec Microsoft Cluster Server (MSCS), ce qui permet de sauvegarder l'ensemble d'un cluster (disques locaux et partagés) et les applications exécutées dans un environnement de type cluster. Pour plus d'informations sur les versions de système d'exploitation prises en charge, les configurations prises en charge et le niveau de prise en charge des clusters, reportez-vous au document *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*.

Nous supposons que vous connaissez bien MSCS. Si tel n'est pas le cas, reportez-vous à la documentation en ligne de MSCS pour plus d'informations.

Attribution de licence et MSCS

Lorsque vous achetez une licence du Gestionnaire de cellule Data Protector, notez que cette licence est liée au serveur virtuel et fonctionne indépendamment du système au sein d'un cluster MSCS qui exécute le Gestionnaire de cellule Data Protector.

Configuration

Vous pouvez configurer l'intégration de deux manières :

- Le Gestionnaire de cellule Data Protector peut être installé sur le serveur MSCS. Ceci procure une plus haute disponibilité du Gestionnaire de cellule Data Protector et permet la migration automatique des services Data Protector d'un nœud cluster vers un autre en cas de basculement, et donc le redémarrage automatique des sessions de sauvegarde ayant échoué.
- Le client Data Protector peut être installé sur MSCS, permettant ainsi les sauvegardes de système de fichiers et les sauvegardes des applications compatibles cluster.

  Pour sauvegarder une application compatible cluster, utilisez le nom de son serveur virtuel lors de la configuration de la spécification de sauvegarde.

REMARQUE :
Les composants Service de cluster (le gestionnaire de base de données, par exemple) maintiennent une image cohérente de la base de données centrale du cluster, qui stocke les informations concernant les modifications apportées à l'état d'un noeud, d'une ressource ou d'un groupe. La base de données du cluster doit être stockée sur le volume de disque partagé du cluster.

Gestion de sauvegardes compatibles cluster

Dans le Gestionnaire de cellule de cluster Data Protector, une session de sauvegarde est compatible cluster. Vous pouvez paramétrer des options qui définissent le comportement relatif à la sauvegarde en cas de basculement de Data Protector ou d'autres applications compatibles cluster.

Basculement de Data Protector

Si un basculement de l'application Data Protector compatible cluster survient pendant la sauvegarde, toutes les sessions de sauvegarde en cours et en attente échouent. Dans l'interface utilisateur graphique Data Protector et dans la spécification de sauvegarde, vous pouvez paramétrer l'une des trois options qui définissent le redémarrage automatique des sessions de sauvegarde en cas de basculement de Data Protector.

Basculement d'une application autre que Data Protector

Étant donné que l'application Data Protector compatible cluster est une application de stockage au sein d'un environnement de type cluster, elle doit connaître les autres applications éventuellement exécutées dans le cluster. Si elles sont exécutées sur un autre nœud que Data Protector et si l'une d'elles bascule sur le nœud sur lequel Data Protector est exécuté, une surcharge se produit sur ce nœud. Ainsi, un nœud qui auparavant gérait uniquement des opérations de sauvegarde se retrouve à gérer également des demandes d'application critiques. Data Protector vous permet de définir ce qui doit arriver dans une telle situation afin que les données d'applications critiques soient protégées et que la charge soit de nouveau partagée.

Vous pouvez effectuer les tâches suivantes:

- Abandonner toutes les sessions de sauvegarde en cours

  Si la sauvegarde est moins importante que l'application, Data Protector peut automatiquement abandonner toutes les sessions en cours pour équilibrer la charge après le basculement de l'application.

  Pour définir cette option, vous devez créer le script approprié avec la commande `omniclus`.
- Désactiver temporairement les activités de sauvegarde

  Si la sauvegarde est moins importante que l'application, Data Protector peut automatiquement désactiver le Gestionnaire de cellule pendant une période donnée pour équilibrer la charge après le basculement de l'application. Toutes les sessions en cours continuent, mais vous ne pouvez pas lancer de nouvelles sauvegardes tant que le Gestionnaire de cellule n'est pas de nouveau activé.

  Pour déterminer cette option, vous devez créer un script approprié avec la commande `omniclus`.
- Abandonner les sessions en cours sur la base du temps de session écoulé

Pour équilibrer la charge après un basculement de l'application, vous pouvez abandonner des sessions de sauvegarde sur la base de leur durée d'exécution actuelle. Si une session de sauvegarde spécifique en cours est sur le point de se terminer, Data Protector peut continuer la session. Si la session de sauvegarde vient juste de commencer et qu'elle n'est pas importante, Data Protector peut l'abandonner.

Pour déterminer l'une de ces options, vous devez créer un script approprié avec la commande `omniclus` et définir les options de sauvegarde en cluster dans le GUI Data Protector.

- Abandonner les sessions en cours sur la base d'un ID logique

  Si une session de sauvegarde en cours est plus importante que l'application, Data Protector peut continuer cette session. Pour équilibrer la charge après un basculement, vous pouvez abandonner toutes les sessions de sauvegarde excepté une sauvegarde importante via son ID d'abandon.

  Pour déterminer cette option, vous devez créer un script approprié avec la commande `omniclus` et définir les options de sauvegarde en cluster dans le GUI Data Protector.

À propos de la récupération après sinistre d'un serveur Microsoft Cluster Server

Il est possible de récupérer Microsoft Cluster Server (MSCS) à l'aide de n'importe quelle méthode de récupération après sinistre, à l'exception de la récupération après sinistre avec restitution de disque. Toutes les spécificités, limitations et exigences propres à une méthode de récupération après sinistre s'appliquent également à la récupération de MSCS. Sélectionnez la méthode de récupération après sinistre qui convient pour votre cluster et incluez-la dans votre plan de récupération après sinistre. Etudiez les limitations et les exigences de chaque méthode de récupération après sinistre avant de prendre votre décision. Exécutez les tests du plan de test.

Pour obtenir des informations sur les systèmes d'exploitation pris en charge, reportez-vous au document *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*.

Toutes les conditions préalables à la récupération après sinistre (sauvegarde cohérente et à jour, fichier DRS à jour, remplacement de tous les matériels défectueux, par exemple) doivent être satisfaites afin de récupérer le MSCS.

Scénarios possibles

Deux scénarios sont possibles pour la récupération après sinistre d'un MSCS :

- un ou plusieurs noeuds ont subi un sinistre ;
- tous les noeuds du cluster ont subi un sinistre.

À propos de l'intégration de HPE Data Protector avec HPE Serviceguard

Pour plus d'informations sur les concepts de gestion de clusters, l'architecture et HPE Data Protector dans un environnement de cluster, consultez le *Guide conceptuel HPE Data Protector*.

Pour plus d'informations sur l'installation de HPE Data Protector dans un environnement de cluster, consultez le *Guide d'installation HPE Data Protector*.

Comme élément de forte disponibilité, Data Protector offre une intégration avec HPE Serviceguard (HPE SG) pour les systèmes HP-UX et Linux, vous permettant de sauvegarder un cluster complet (disques locaux et partagés) et des applications fonctionnant dans un environnement de cluster. Pour plus d'informations sur les versions de système d'exploitation prises en charge, les configurations prises en charge et le niveau de prise en charge des clusters, reportez-vous au document *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*.

Vous êtes censé être familier avec HPE Serviceguard. Au sinon, consultez le manuel *Gérer HPE Serviceguard* pour obtenir de plus amples informations.

Licence et HPE Serviceguard

Lorsque vous achetez une licence pour le Responsable de Cellule Data Protector, veuillez noter que le licence sera liée au serveur virtuel et fonctionnera peu importe quel noeud physique à l'intérieur d'un cluster HPE SG exécute le package de clusters Data Protector, aussi longtemps que le package fonctionne sur un des nœuds.

Configuration

Vous pouvez configurer l'intégration de deux manières :

- Le Responsable de Cellule Data Protector peut être installé dans HPE SG. Ceci permet la migration automatique des services Data Protector d'un nœud cluster vers un autre en cas de basculement, et donc le redémarrage automatique des sessions de sauvegarde ayant échoué.

  Le nœud de cluster inactif peut également être utilisé comme serveur d'installation.
- Le client Data Protector en grappes peut être installé dans HPE SG prenant donc en charge les sauvegardes du système de fichiers et les sauvegarde des applications en grappes.

A propos de l'intégration de HPE Data Protector avec IBM HACMP Cluster

Pour plus d'informations sur les concepts de gestion de clusters, l'architecture et HPE Data Protector dans un environnement de cluster, consultez le *Guide conceptuel HPE Data Protector*.

Pour plus d'informations sur l'installation de HPE Data Protector dans un environnement de cluster, consultez le *Guide d'installation HPE Data Protector*.

Le logiciel IBM HACMP est la solution d'IBM pour créer des environnements informatiques stratégiques sous UNIX, sur la base des concepts de haute disponibilité (High Availability ou HA) et de multitraitement de cluster (Cluster Multi-Processing ou CMP). Cette solution garantit la disponibilité pour traitement des ressources critiques telles que les applications.

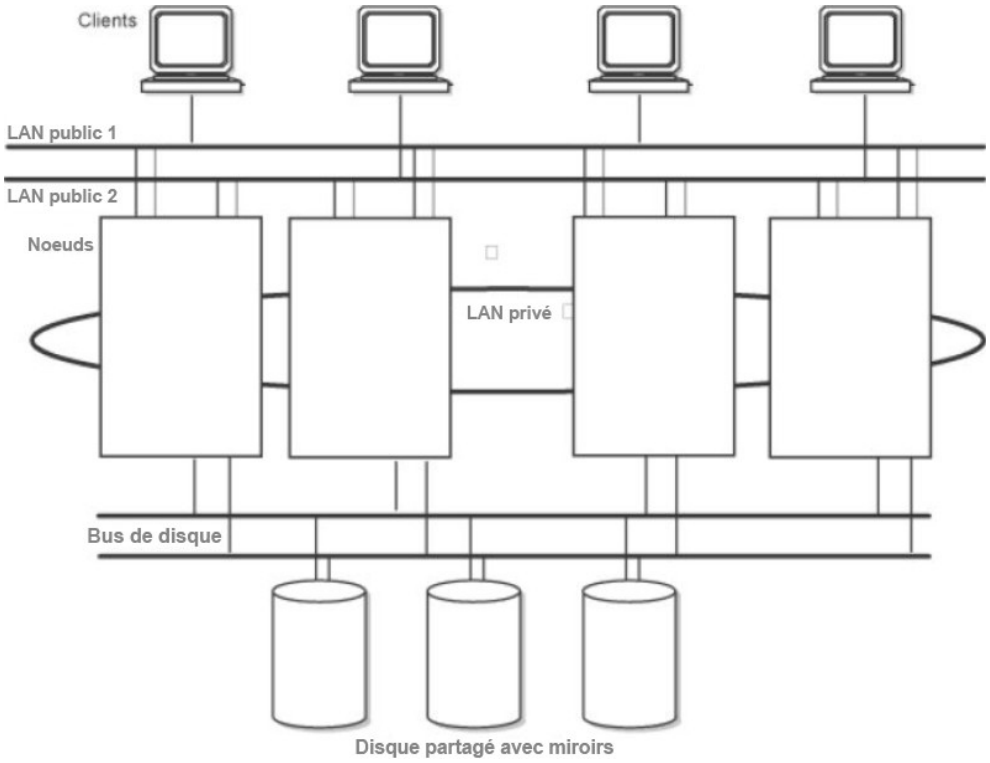
La création de clusters HACMP a pour objectif principal de fournir un environnement à haute disponibilité pour les applications stratégiques. Par exemple, un cluster HACMP peut exécuter un programme de serveur de base de données qui est utilisé par des applications clientes. Ces dernières envoient des requêtes au programme de serveur qui y répond en accédant à une base de données, stockée sur un disque externe partagé.

Pour garantir la disponibilité de ces applications dans un cluster HACMP, elles sont placées sous le contrôle du logiciel IBM HACMP. Celui-ci veille à maintenir la disponibilité des applications pour les

processus clients, même en cas de défaillance d'un élément d'un cluster. Dans ce cas, le logiciel HACMP déplace l'application (ainsi que les ressources qui assurent l'accès à l'application) vers un autre nœud du cluster.

Le cluster est intégralement accessible via un nom de serveur virtuel (le Nom de Domaine de l'Environnement Virtuel), qui représente le cluster HACMP sur le réseau.

Installation typique de cluster HACMP



Comme l'indique la figue, un cluster HACMP est constitué des éléments physiques suivants :

- Nœuds
- Interfaces de disques externes partagés
- Réseaux
- Interfaces réseau
- Clients

Nœuds

Les nœuds forment le cœur d'un cluster HACMP. Chaque nœud est identifié par un nom unique, et contient un processeur qui exécute le système d'exploitation AIX, le logiciel HACMP et le logiciel d'application. Un nœud peut posséder un ensemble de ressources-disques, de groupes de volumes, de systèmes de fichiers, de réseaux, d'adresses réseau et d'applications.

Interfaces de disques externes partagés

Chaque nœud a accès à un ou plusieurs périphériques sur disques externes partagés (disques reliés physiquement à plusieurs nœuds). Les disques partagés stockent des données stratégiques, avec généralement une mise en miroir ou une configuration RAID pour la redondance des données. Notez que les nœuds d'un cluster HACMP possèdent également des disques internes qui stockent le système d'exploitation et les exécutables de l'application, mais ces disques ne sont pas partagés.

Réseaux

En tant qu'élément indépendant basé sur le système d'exploitation AIX, le logiciel HACMP est conçu pour fonctionner avec un réseau TCP/IP. Le réseau sert à:

- permettre aux clients d'accéder aux nœuds du cluster,
- permettre aux nœuds du cluster d'échanger des messages de pulsation,
- sérialiser l'accès aux données (dans des environnements à accès simultané).

Le logiciel HACMP définit deux types de réseaux de communication, selon qu'ils utilisent des interfaces de communication basées sur le sous-système TCP/IP (réseau TCP/IP) ou un autre sous-système (réseau de périphériques).

Clients

Un client est un processeur qui peut accéder aux nœuds d'un cluster via un LAN. Chaque client exécute une application frontale ou cliente

qui interroge l'application du serveur exécutée sur le nœud du cluster.

Tâches

Installation et configuration de l'intégration de Data Protector avec IBM HACMP Cluster

Chapitre 7: Contexte d'accueil

Avec Data Protector 10.00, l'interface utilisateur reçoit un nouveau contexte de gestion, lequel offre une méthode unifiée pour accéder au **Tableau de bord**, à la **Télémétrie** et au **Planificateur** Web.

Tableau de bord

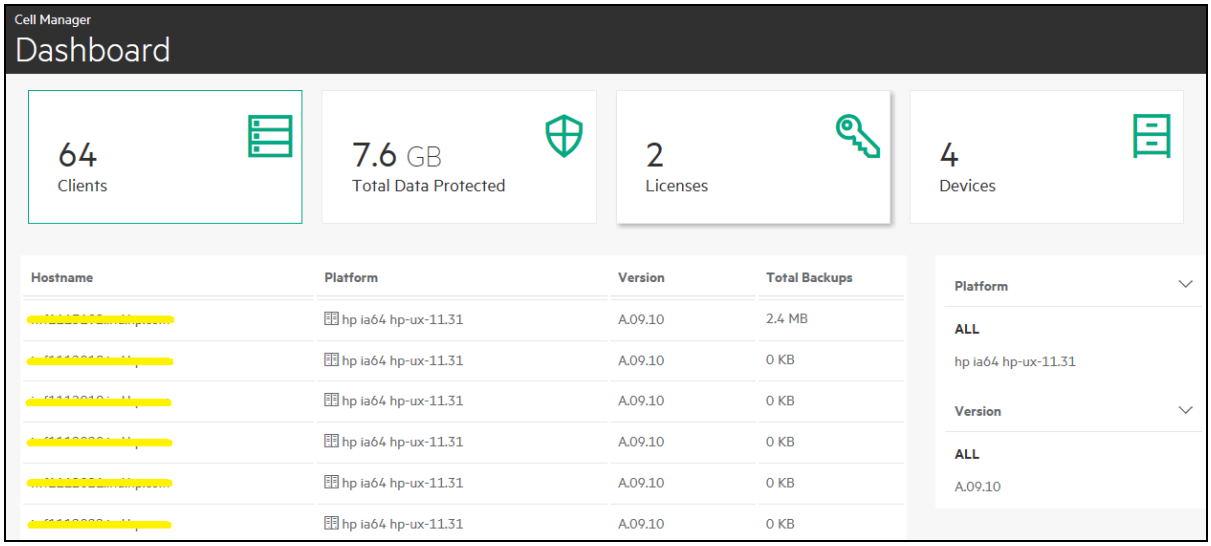
La page de tableau de bord fournit à l'utilisateur une vue d'ensemble de l'instance Gestionnaire de cellule, en détaillant le total des données protégées, les clients disponibles, les périphériques de stockage et les licences installées.

Comment accéder à la page Tableau de bord ?

Pour accéder à la page Tableau de bord, cliquez sur le menu contextuel **Accueil** dans l'interface utilisateur, puis sur Tableau de bord dans le volet de gauche.

La page de tableau de bord se divise en quatre catégories :

- Clients
- Données totales protégées
- Licences
- Périphériques



Clients

La liste des clients répertorie tous les clients actuellement configurés avec le nom d'hôte, le système d'exploitation, la version et le nombre total de sauvegardes.

- **Nom d'hôte** : cette colonne fournit la liste de tous les noms d'hôte des clients disponibles. Les noms d'hôte peuvent être triés par ordre croissant ou décroissant selon les préférences.

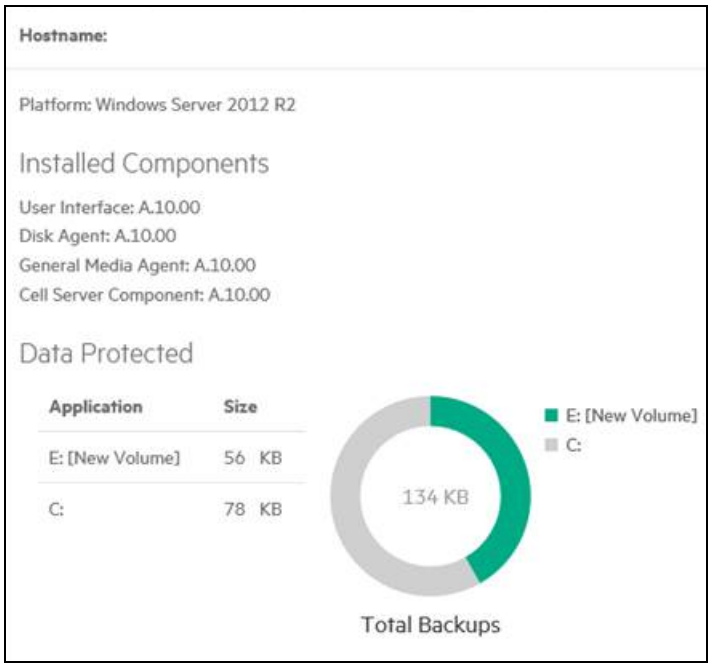
  Lorsque l'utilisateur clique sur la ligne, la boîte de dialogue **Détails supplémentaires sur le client** s'affiche en indiquant des informations sur les composants installés et la sauvegarde d'applications. La

sauvegarde s'affiche sous la forme d'un graphique dans lequel figurent les différentes sauvegardes d'applications.

- **Plate-form**e : cette colonne dresse la liste de tous les systèmes d'exploitation utilisés par les clients. La partie droite de la page comporte des filtres supplémentaires permettant d'afficher les clients dotés d'un système d'exploitation particulier.
- **Version** : cette colonne dresse la liste des numéros de version du gestionnaire de cellule ou du client. La partie droite de la page comporte des filtres supplémentaires permettant d'afficher les clients dotés d'une version particulière.
- **Nombre total de sauvegardes** : cette colonne dresse la liste des sauvegardes totales effectuées sur chaque client.

Données totales protégées

Totalité des données protégées sur l'instance Gestionnaire de cellule. Les données sont affichées sous forme de graphique avec la quantité de données sauvegardées pour le type de données (système de fichier) correspondant.



Licences

Le nombre de licences installées sur chaque système. Ces entrées sont classifiées plus en détail comme suit :

- **Licences en ligne** : une licence en ligne est un mécanisme d'attribution de licence qui vous permet d'obtenir des licences pour une période.
- **Licences en capacité** : une licence en capacité est un mécanisme d'attribution de licences qui vous permet d'obtenir des licences en fonction du volume de données que vous sauvegardez.

Périphériques

Dresse la liste de tous les périphériques de stockage de l'instance Gestionnaire de cellule.

Ces entrées sont classifiées plus en détail comme suit :

- **Nom d'hôte** : cette colonne indique le nom d'hôte du périphérique ou du serveur de médias. Les entrées peuvent être triées par ordre croissant ou décroissant selon les préférences.
- **Nom de la bibliothèque** : cette colonne dresse la liste de tous les noms de bibliothèque associés aux périphériques de stockage.
- **Périphérique** : cette colonne dresse la liste des types de périphériques de stockage. La partie droite de la page comporte une option permettant à l'utilisateur de filtrer les colonnes suivant le type de périphérique spécifique.
- **Type** : cette colonne dresse la liste des types de périphériques de stockage.
- **Nom du pool** : cette colonne dresse la liste de tous les pools de supports associés aux périphériques de stockage.
- **Utilisation** : capacité du périphérique utilisé pour sauvegarder les données.

Télémétrie

Le service de client de télémétrie Data Protector collecte les données depuis le Data Protector Gestionnaire de cellule par le biais du Serveur d'application et télécharge les données télémétriques qu'il envoie au soutien HPE Data Protector à des fins d'analyse.

Comment accéder à la page de Télémétrie ?

Pour accéder à la page de télémétrie, cliquez sur le menu de contexte **Accueil** dans l'interface utilisateur graphique, puis cliquez sur Télémétrie dans le panneau de gauche.

Le service de client de télémétrie est un service Windows et Linux qui est déployé sur un client de Console de cellule (CC). La page de service affiche le service de client de télémétrie Data Protector où l'utilisateur peut commencer ou arrêter le service.

Data Protector collecte les informations de haut niveau suivantes pour la télémétrie :

- Informations sur les composants - composants Data Protector et leurs versions. Elles fournissent également des informations sur la version SE host.
- Dispositifs ou Serveurs de Support - les détails associés à un client dans le Responsable de Cellule qui comprennent les détails de nom de l'host qui a la date d'utilisation du dispositif jointe, le nom du dispositif, qui a la taille d'utilisation de dispositif jointe, nom du dispositif, nom de bibliothèque, type de dispositif et nom de pool lorsque le support est placé.
- Taille d'utilisation du dispositif – La taille d'utilisation du dispositif
- Licence basée sur la capacité (LBC) : La LBC est exploitée pour regrouper des informations sur la capacité. Pour plus de détails, consultez le *Guide d'installation HP Data Protector*.
- Catégories de licence classiques : elles fournissent des informations sur les licences installées sur chaque hôte et les licences disponibles.
- Utilisation des clients (informations collectées pour chaque client). Ces informations comprennent : le nom de l'host, le nom de l'application et la taille totale des données sauvegardées.
- Utilisation du stockage (total des données sauvegardées sur le périphérique).

Conditions préalables

- Le service de client de télémétrie déployé sur CC doit être configuré avec un proxy afin de pouvoir communiquer avec le serveur dorsal de soutien HPE.

- Lors de la configuration de la télémétrie, le nom d'utilisateur et les informations de proxy doivent être disponibles.

> **REMARQUE :**
> Les informations liées au client sont regroupées, mais les informations liées à l'hôte sont masquées.
>
> La performance du responsable de Cellule n'est pas impactée pendant la collecte des données télémétriques.

Restrictions :

- Le service de client de télémétrie n'est compatible qu'avec les systèmes d'exploitation Windows x64 et Linux x64.

Comment la télémétrie fonctionne-t-elle ?

Au cours de l'enregistrement de la télémétrie, les informations sont stockées dans l'IDB. Tout hôte Windows où le composant d'interface utilisateur graphique DP est installé est un client de télémétrie approprié. Selon la fréquence de téléchargement configurée, le client de Console de cellule (CC) contrôle les paramètres de l'IDB et récupère les données de télémétrie depuis le Gestionnaire de cellule et les télécharge sur le serveur de back-end.

Si le service est hors ligne pendant le processus de collecte, le téléchargement de télémétrie ne s'effectue pas à ce moment. Lorsque le service est en ligne, le client devient éligible au téléchargement des données de télémétrie.

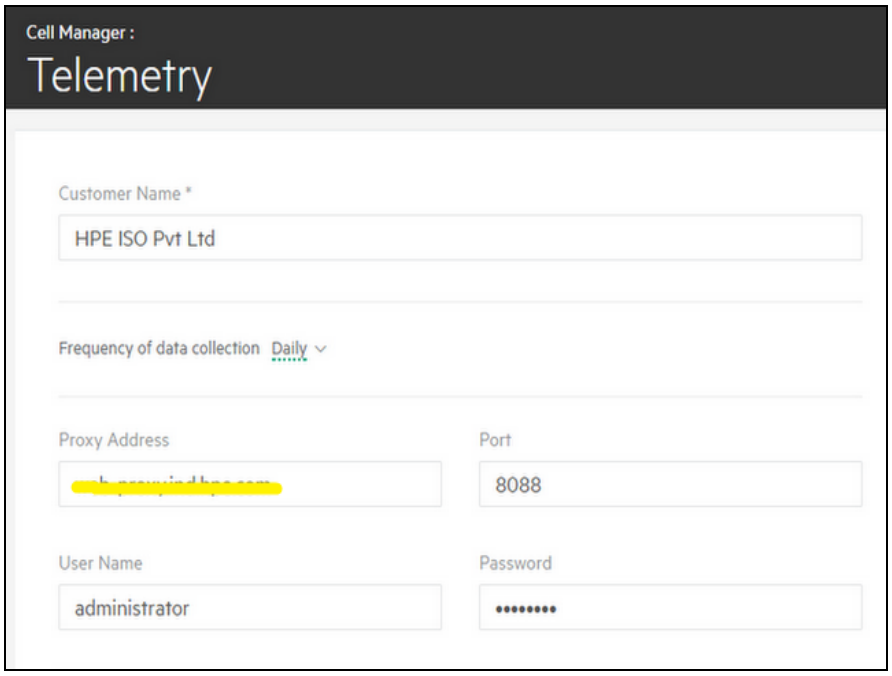
Dans une cellule, si plusieurs clients de télémétrie cohabitent, un seul client effectue le téléchargement vers le back-end en fonction de la fréquence de téléchargement. L'IDB est mise à jour avec l'état et l'heure du téléchargement.

Depuis les clients de télémétrie, si un proxy est nécessaire pour accéder au réseau externe, vous devez spécifier les paramètres de proxy. Ceci est inutile dans le cas où une connexion directe est possible.

Page de Télémétrie

L'utilisateur peut s'inscrire ou se désinscrire des mises à jour de télémétrie via la page Télémétrie. Pour s'inscrire aux mises à jour de télémétrie, entrez les champs suivants :

- **Nom du client** : le nom du client.
- **Fréquence de collecte des données** : l'utilisateur peut sélectionner la périodicité (quotidienne, hebdomadaire, mensuelle ou trimestrielle) selon laquelle les données sont collectées.
- **Proxy** [optionnel] : l'adresse du serveur proxy configuré.
- **Port** [Optionnel] : le port du serveur proxy.
- **Nom d'utilisateur** [Optionnel] : nom d'utilisateur de connexion au serveur proxy.
- **Mot de passe** [Optionnel] : mot de passe associé au nom d'utilisateur.



Après avoir renseigné les champs ci-dessus et sélectionné la fréquence de collecte des données, acceptez les conditions générales, puis cliquez sur **S'inscrire**.

Planificateur

> **IMPORTANT :**
> Avec Data Protector 10.00, les planificateurs de base et avancé sont obsolètes, et remplacés par un nouveau planificateur Web. Pendant la mise a niveau, toutes vos planifications existantes sont automatiquement migrees vers le nouveau planificateur.

Data Protector 10.00 est doté d'un tout nouveau planificateur muni d'une interface utilisateur améliorée et de commandes web simplifiées et faciles d'utilisation, qui facilite la gestion de planification. Vous pouvez maintenant definir la priorite de planification, la protection des donnees et le schema de recurrence et resoudre les conflits a l'aide d'un seul et meme assistant Planifier.

Utilisez le planificateur pour automatiser diverses opérations, comme la sauvegarde, la copie de supports, la consolidation et la copie d'objets, à des intervalles réguliers. L'exécution sans surveillance, en arrière-plan, de ces opérations élimine la nécessité de répéter manuellement une planification à chaque fois que vous voulez lancer une opération.

Comment accéder à la page du Planificateur ?

Pour accéder à la page du planificateur, cliquez sur le menu contextuel **Accueil** dans l'interface utilisateur graphique, puis cliquez sur **Planificateur** dans le panneau de gauche.

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, l'Assistance HPE 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.
- Au cours de la mise à niveau, les planifications minutes/heures/années configurées dans des versions antérieures de Data Protector ne migreront pas vers Data Protector 10.00.

Options de planification

Selon le type de spécification, vous pouvez paramétrer les options de planification suivantes :

- Type de sauvegarde : le type de sauvegarde, complète ou incrémentale.
- Charge réseau : la charge réseau voulue pour la session. La définition de cette option sur **Moyenne** or **Bas** permet de réduire la charge réseau lorsque vous exécutez Data Protector. Ainsi, le processus de transmission des données ne bloque pas l'accès des autres utilisateurs au réseau, mais le temps d'exécution de la session est plus important.
- Protection des données : la période de protection des données sauvegardées pour éviter que la sauvegarde ne soit écrasée.
- Modèle de récurrence ; la fréquence à laquelle la planification s'exécute.
- Durée estimée : la durée estimée de votre session, qui détermine l'affichage des planifications dans le calendrier.

Dans le cas de ZDB sur disque + bande ou ZDB sur disque (si la restauration instantanée est activée), spécifiez l'option **Sauvegarde Split Mirror/Snapshot**.

Chaque spécification de sauvegarde peut être planifiée plusieurs fois avec différentes options. Dans une spécification de sauvegarde, vous pouvez planifier à la fois des sessions ZDB sur disque et ZDB sur disque + bande, et spécifier une période de protection des données différente pour chaque sauvegarde planifiée individuelle ou périodique.

Le nouveau Planificateur dispose également des fonctionnalités suivantes :

Suspension des planifications les jours chômés

Vous pouvez définir différents jours chômés en modifiant le fichier Holidays situé sur le répertoire de configuration de serveur Data Protector par défaut.

Par défaut, Data Protector exécute les sauvegardes les jours chômés. Si vous voulez modifier le comportement par défaut, appuyez-vous sur l'exemple suivant. Si la date du 1er janvier est inscrite comme un jour chômé, Data Protector n'effectue aucune sauvegarde à cette date. Si vous avez planifié une sauvegarde complète le 1er janvier et une sauvegarde incrémentale le 2 janvier, Data Protector ignorera la sauvegarde complète le 1er janvier mais exécutera la sauvegarde incrémentale planifiée le 2 janvier. La sauvegarde incrémentale sera basée sur la dernière sauvegarde complète.

Prenez en compte les éléments suivants lorsque vous éditez ou ajoutez de nouvelles entrées dans le fichier `Holidays`:

- Le premier chiffre de chaque ligne indique le jour consécutif de l'année. La valeur est ignorée par Data Protector, mais doit être définie entre `0` et `366`. Vous pouvez la définir sur `0` pour indiquer que le nombre ne correspond pas à la date qui suit.

- La date est spécifiée comme `Mmmd`, où `Mmm` est l'abréviation à trois lettres du mois et `d` le jour du mois sous forme de nombre (par exemple, `Jan 1`). Notez que le mois doit être indiqué en anglais, quels que soient vos paramètres linguistiques.
- La description du jour chômé est facultative et n'est actuellement pas utilisée par Data Protector.

Quelle que soit l'année spécifiée au début du fichier, les jours chômés spécifiés dans le fichier sont toujours utilisés tels quels et doivent être modifiés manuellement s'ils ne tombent pas aux mêmes dates chaque année. Si vous n'utilisez pas l'option **Jours chômés** pour le planificateur, vous pouvez supprimer ou désactiver par un commentaire les entrées du fichier `Holidays` pour éviter toute confusion en cas d'utilisation accidentelle d'un fichier `Holidays` obsolète ou n'ayant pas été personnalisé selon les besoins spécifiques de votre pays ou de votre entreprise.

Utiliser des planifications prédéfinies

Le Planificateur Data Protector est doté d'une série de planifications prédéfinies qui simplifient la configuration des planifications. Vous pouvez modifier ces planifications ultérieurement.

Gestion des conflits de planifications

Lors de la planification de sauvegardes périodiques, il se peut que la tranche horaire choisie pour la sauvegarde soit déjà occupée par une autre sauvegarde planifiée dans la même spécification de sauvegarde. Dans ce cas, l'assistant de planification Data Protector vous indique qu'il existe des conflits de planifications. Vous pouvez redéfinir le modèle de récurrence, ou permettre au planificateur de paramétrer la planification sur des jours où des tranches horaires sont toujours disponibles. En fonction de la disponibilité des tranches horaires, les valeurs suivantes sont paramétrées en tant que statut de planification :

- Active : la planification n'a pas de conflit, et s'exécutera à l'heure planifiée.
- Chevauchement : la planification est en état de conflit, mais des tranches horaires sont encore disponibles le jour sélectionné, où la planification peut s'exécuter.
- Inactive : la planification est en état de conflit, et aucune tranche horaire n'est plus disponible le jour sélectionné, où la planification peut s'exécuter.
- Désactivée : la planification a été explicitement désactivée par l'utilisateur.

Planification dans différents fuseaux horaires

Toutes les planifications sont affichées dans le calendrier avec le fuseau horaire du système du Gestionnaire de cellule. Si vous avez spécifié une session de sauvegarde ou d'opérations sur objet pour un fuseau horaire autre que celui du Gestionnaire de cellule, la session sera exécutée à l'heure indiquée dans le fuseau horaire spécifié.

Prioriser les planifications

Vous pouvez établir une priorité pour chaque planification, à l'aide de l'assistant de planification. Dans le cas où plusieurs sessions en cours d'exécution requièrent un accès à un périphérique spécifique en même temps, la priorité détermine l'ordre dans lequel les sessions seront mises en attente. La priorité peut être définie pour chaque planification.

- Vous pouvez spécifier qu'une session planifiée peut mettre en pause d'autres sessions dont la priorité est inférieure à celle de la session sélectionnée.

  > **REMARQUE :**
  > Les options Planification des tâches de priorité et Mise en pause des tâches de priorité inférieure ne sont pas prises en charge dans l'environnement CMMDB.

- La possibilité de mettre en pause une session et de la reprendre là où elle s'est arrêtée est disponible dans les sessions d'intégration de système de fichiers, VMware et Oracle Server. Pour d'autres intégrations, après la mise en attente, la session de sauvegarde redémarre.
- Les sessions de sauvegarde Backup to Disk (B2D) ne peuvent pas être suspendues en fonction d'une priorité.
- Pour les sessions de sauvegarde contenant une combinaison de types de périphériques de sauvegarde, par exemple une bibliotheque de fichiers et un systeme B2D, la fonctionnalité de suspension s'applique uniquement aux périphériques non-B2D.
- Le planificateur maintient une file d'attente de tâches internes pour gérer les priorités. Si les tâches multiples partagent la même bibliothèque de fichier que le périphérique cible, le planificateur n'affichera qu'une tâche à la fois, et il n'affichera que la suivante lorsque la précédente se terminera et libèrera le périphérique. La tâche avec la priorité la plus élevée sera envoyée en premier. Si les multiples tâches ont la même priorité, alors celle avec l'heure de planification la plus proche sera envoyée en premier. Si elles ont la même priorité et la même heure de planification, alors l'une d'elles sera choisie aléatoirement et envoyée.

Exemple de planification et de priorité

Voici un exemple de la manière dont le planificateur gère les sessions de sauvegarde en se basant sur la priorité et la pause.

Il y a trois sessions à planifier, où :

- `Job1` a une priorité de 2000 avec l'option **Mise en pause des tâches de priorité inférieure** activée.
- `Job2` a une priorité de 4000.
- `Job3` a une priorité de 3000 avec l'option **Mise en pause des tâches de priorité inférieure** activée.

1. `Job2` est en cours d'exécution.
2. Planifiez `Job1` et `Job3` pour le même moment. La session `Job1` a la possibilité de mettre en pause d'autres sessions activées. Aussi, la session `Job2` sera mise en pause en faveur de `Job1`.
3. Une fois la session `Job1` terminée, la session `Job3` s'exécute.

   La session `Job2` mise en pause reste en pause jusqu'à ce qu'elle soit capable de s'exécuter en fonction de la planification et de la priorité. Cette session peut ne jamais avoir l'occasion de se lancer, s'il y a d'autres sessions avec une priorité supérieure.

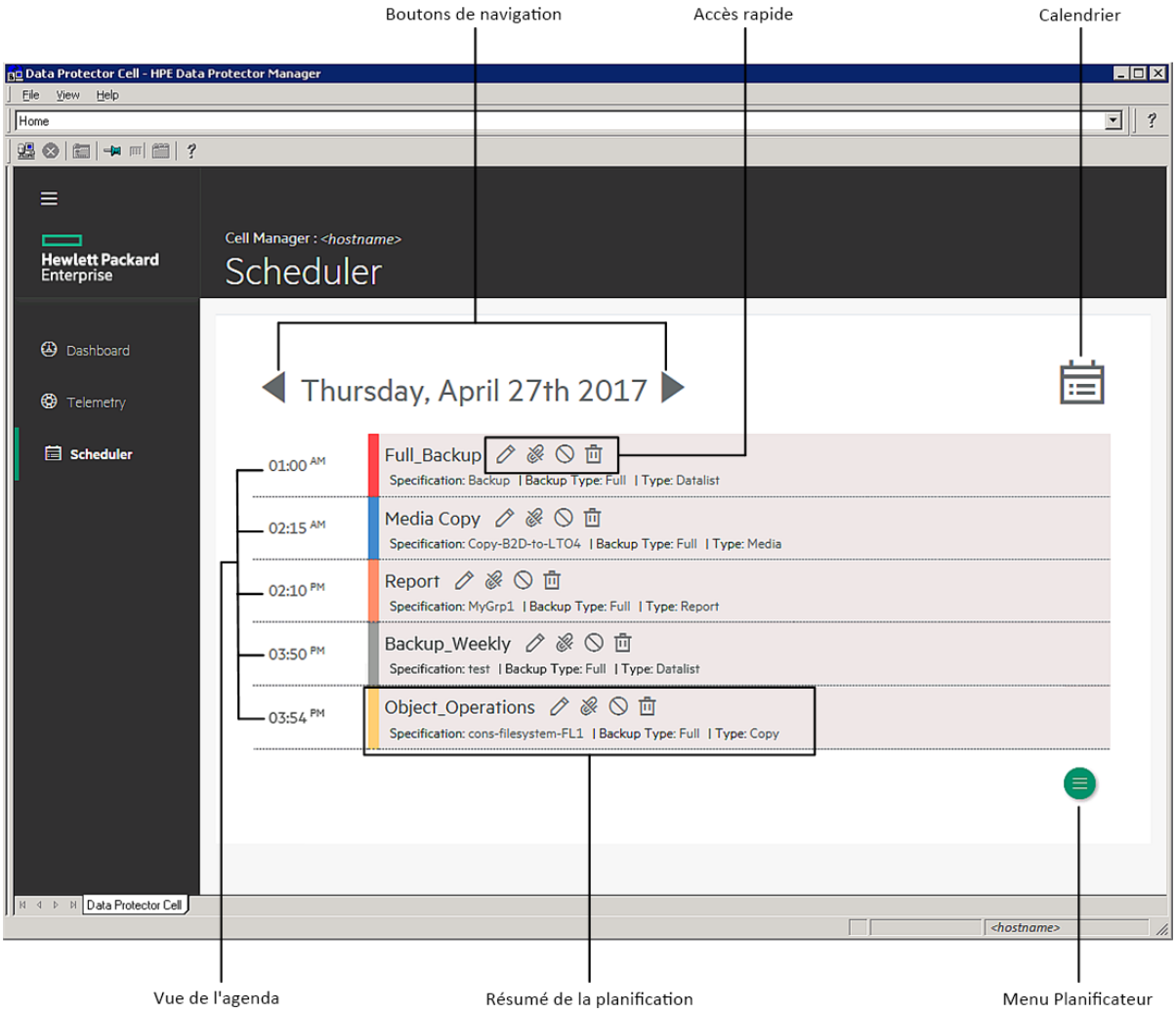
Limites

Le planificateur Data Protector fait l'objet des restrictions suivantes :

- Restriction du navigateur : Pour que la page Planificateur fonctionne, Microsoft Internet Explorer 11 doit être installé sur l'ordinateur.

Interface utilisateur du planificateur

L'image ci-dessous présente l'interface utilisateur du planificateur et les diverses commandes qui apparaissent sur cette page.



Toutes les commandes sont détaillées dans le tableau ci-dessous :

Contrôle	Description
Boutons de navigation	Les boutons de navigation **Précédent** et **Suivant** qui vous permettent d'avancer ou de reculer la date, et de voir l'agenda pour la date sélectionnée.
Accès rapide	Une série d'icônes, disponibles pour chaque planification, qui offre des raccourcis vers les opérations couramment utilisées du

	planificateur.  • Modifier : ouvre l'assistant de planification, et vous permet de modifier tous les paramètres disponibles pour la planification. • Désactiver l'instance : désactive l'instance sélectionnée, pour la date sélectionnée. S'il s'agit d'une planification récurrente, seule l'instance sélectionnée est désactivée. Lorsque vous désactivez une instance, la planification est supprimée de l'agenda du jour concerné. • Désactiver série : désactive toutes les instances de la planification. Si vous désactivez la planification, la planification s'affiche en couleur grise. Désactiver une planification n'a aucun impact sur les éventuelles planifications en cours. • Supprimer : supprime la planification.
Calendrier	Affiche le calendrier Vous pouvez sélectionner une date dans le calendrier, et l'agenda de cette date s'affiche.
Vue de l'agenda	Liste toutes les planifications de la date sélectionnée, y compris les planifications désactivées.
Résumé de la planification	Fournit un résumé de la planification. Par exemple, vous pouvez voir le nom de la spécification pour laquelle la planification a été créée, le type de sauvegarde (complète / incrémentale) qui doit être effectuée, et le type de planification. Le code couleur placé à côté de chaque planification signifie son **Type** : • Le rouge indique que la planification a été créée pour une opération de sauvegarde. • Le bleu indique que la planification a été créée pour une opération de support. • Le orange indique que la planification a été créée pour la génération de rapports. • Le jaune indique que la planification a été créée pour une opération de copie. • Le gris indique que la planification est désactivée.
Menu du planificateur	Le menu du planificateur qui vous permet de créer une nouvelle planification.

Tâches du planificateur

Le planificateur vous permet d'effectuer les tâches suivantes.

- Création d'une planification
- Modification d'une planification existante

- Affichage d'une planification
- Désactivation et activation d'une planification
- Désactivation et activation d'une planification les jours chômés
- Définition d'une planification à une date et une heure spécifiques
- Définition périodique d'une planification

OBSOLÈTE :
Le nouveau planificateur Web ne permet pas de réinitialiser les planifications. L'option de réinitialisation de planification était utilisée pour effacer tous les paramètres de planification de l'année courante dans la spécification.

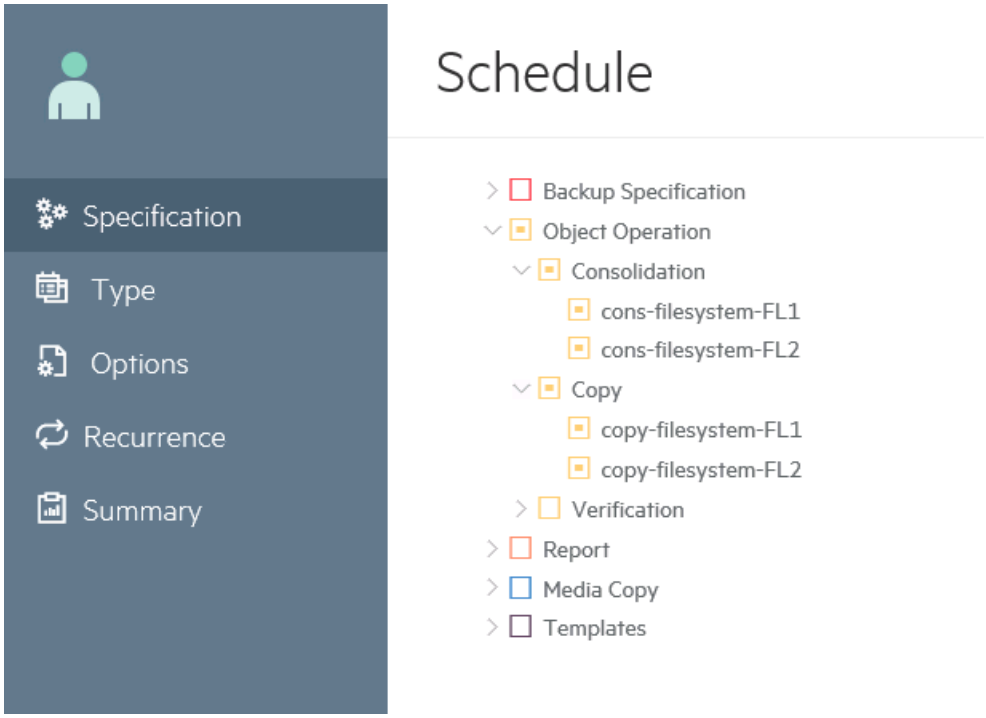
Création d'une planification

Exécutez les étapes suivantes pour créer une planification.

Les étapes de cette procédure expliquent comment créer une planification de spécification de sauvegarde. Les options disponibles dans l'assistant de planification sont basées sur les types de spécifications que vous choisissez.

1. Dans le menu de contexte, cliquez sur **Accueil**, puis sur **Planificateur** dans le panneau de gauche. La page du Planificateur s'affiche.
2. Cliquez sur l'icône de menu du planificateur dans le coin en bas à droite de la page du planificateur, puis cliquez sur l'icône ajouter pour ouvrir l'assistant de planification. La page Spécifications s'affiche.
3. Choisissez le type de spécification pour lequel vous souhaitez créer une planification.

   Par exemple, l'image ci-dessous montre l'arbre développé des Opérations sur les objets, avec une liste des opérations pour lesquelles vous pouvez créer des planifications : consolidation, copie, et vérification.



Cliquez sur **Modèles** si vous souhaitez ajouter une planification à un modèle existant.

Vous pouvez ensuite appliquer ce modèle à une spécification depuis le menu Sauvegarde. Une fois un modèle appliqué, toutes les planifications au sein de ce modèle sont activées pour la spécification.

Notez que vous ne pouvez utiliser cet assistant pour planifier un modèle.

Cliquez sur **Suivant**. La page Type s'affiche.

4. Cliquez sur le type de planification.
   - Cliquez sur **Personnalisé** pour créer vos propres planifications.
   - Cliquez sur **Prédéfini** pour utiliser l'une des planifications prédéfinies disponibles dans Data Protector. Sélectionnez l'une des propositions suivantes :
     - Intensive - Quotidienne : Data Protector lance une sauvegarde complète à minuit et deux sauvegardes incrémentales à 12h00 (midi) et 18h00 (6 pm) chaque jour.
     - Complète - Quotidienne : Data Protector lance une sauvegarde complète chaque jour à 21h00 (9 pm).
     - Complète - Hebdomadaire : Data Protector lance une sauvegarde complète chaque vendredi et des sauvegardes Incr1 chaque jour du lundi au vendredi à 21h00 (9 pm).
     - Complète - Tous les 15 jours : Data Protector lance une sauvegarde complète un vendredi sur deux. Entre ces sauvegardes, Data Protector lance des sauvegardes Incr1 tous les jours, du lundi au jeudi, à 21h00 (9 pm).
     - Complète - Mensuelle : Data Protector lance une sauvegarde complète tous les mois, une sauvegarde Incr1 toutes les semaines, et une sauvegarde incrémentale un jour sur deux.

   Cliquez sur **Suivant**. La page Options s'affiche.
5. Tapez un nom pour votre planification dans la boîte de texte **Nom de planification**.

6. Sélectionnez le type de **Sauvegarde**, Complète ou Incrémentale. Pour plus d'informations sur les différents types d'options de sauvegarde, consultez la section Types de sauvegardes.
7. Sélectionnez le **Niveau de protection**. Le niveau de protection détermine la durée pendant laquelle les informations sur les données sauvegardées sont conservées dans l'IDB. En l'absence de protection de catalogue, vous pouvez restaurer les données mais pas les parcourir via l'interface Data Protector. Sélectionnez l'une des options suivantes.
   - Aucune : Ne définit aucune protection.
   - Valeur par défaut : Les informations stockées dans la base de données interne sont protégées contre l'écrasement tant que les données sont protégées.
   - Jusqu'au : Les informations de l'IDB ne sont pas écrasées avant la date spécifiée. La protection des données s'arrête le jour indiqué à midi.
   - Jours : Les informations de l'IDB ne sont pas écrasées pendant le nombre de jours spécifié.
   - Semaines : Les informations de l'IDB ne sont pas écrasées pendant le nombre de semaines spécifié.
   - Permanent : Les informations de l'IDB sont disponibles de manière permanente.
8. Déplacez le curseur pour définir la priorité, ou entrez un nombre dans la boîte de texte **Priorité** si le nombre de priorité est supérieur aux valeurs du curseur. Le niveau de priorité est considéré si plusieurs sessions essaient d'accéder à un périphérique au même moment. Dans ce cas, cette option détermine l'ordre dans lequel les sessions seront mises en attente.

   Si une session de priorité inférieure est en cours lorsqu'une session de priorité supérieure est mise en file d'attente, la session en cours est autorisée à se terminer. Lorsque plusieurs sessions avec la même priorité demandent l'accès à un périphérique, chacune de ces sessions peut obtenir l'accès en premier.
9. Spécifiez la **charge réseau**. La définition de cette option sur Moyenne or Bas permet de réduire la charge réseau lorsque vous exécutez Data Protector. Ainsi, le processus de transmission des données ne bloque pas l'accès des autres utilisateurs au réseau, mais le temps d'exécution de la session est plus important.
10. Mettez l'option **Mise en pause des tâches de priorité inférieure** sur ON, si la session planifiée doit être en mesure de pouvoir mettre n pause des sessions de priorité inférieure sur un périphérique occupé. Cette option est utile si plusieurs sessions tentent d'accéder en même temps à un périphérique. Dans ce cas, l'option spécifie que la session sélectionnée peut suspendre d'autres sessions jusqu'à ce qu'elle se termine. Une fois la session terminée, les sessions suspendues reprennent jusqu'à leur terme.

    REMARQUE :
    Cette fonctionnalité est disponible uniquement pour les sessions d'intégration de système de fichiers, VMware et Oracle Server. Les sessions de sauvegarde Backup to Disk (B2D) ne peuvent pas être suspendues en fonction d'une priorité. Pour les sessions de sauvegarde contenant une combinaison de types de périphériques de sauvegarde, par exemple une bibliothèque de fichiers et un système B2D, la fonctionnalité de suspension s'applique uniquement aux périphériques non-B2D.

11. La planification est activée par défaut. Mettez l'option **Planification activée** sur OFF pour désactiver la planification.
12. Mettez l'option **Jours chômés** sur ON si vous souhaitez que les opérations soient lancées également les jours chômés. Pour spécifier différents jours comme jours chômés, modifiez le fichier des jours chômés.

    Cliquez sur **Suivant**. La page Récurrence s'affiche.
13. Sous Modèle de récurrence, indiquez la fréquence des sauvegardes. Sélectionnez le modèle et la fréquence parmi les options suivantes :
    - **Une fois**: La planification s'effectue une seule fois à la date spécifiée. Vous pouvez sélectionner la date de début, le fuseau horaire, et l'heure à laquelle la planification doit débuter.
    - **Quotidienne** : La planification s'effectue régulièrement, à l'heure spécifiée. Vous pouvez spécifier la fréquence de la planification en utilisant le champ Tous les <valeur> Jour(s). Par exemple, une valeur de récurrence de 4 signifie que la planification s'effectuera tous les quatre jours.

      Vous pouvez sélectionner la date de début, le fuseau horaire, et l'heure à laquelle la planification doit débuter.
    - **Hebdomadaire** : La planification s'effectue chaque semaine, le jour spécifié. Vous pouvez spécifier la fréquence de la planification en utilisant le champ Toutes les <valeur> Semaine(s). Par exemple, une valeur de récurrence de 2 signifie que la planification s'effectuera toutes les deux semaines, le jour indiqué.

      Vous pouvez sélectionner la date de début, le fuseau horaire, et l'heure à laquelle la planification doit débuter.
    - **Mensuelle** : La planification s'effectue chaque mois, le jour spécifié. Vous pouvez spécifier la fréquence de la planification en utilisant le champ Tous les <valeur> Mois. Par exemple, une valeur de 2 signifie que la planification s'effectuera tous les deux mois, le jour indiqué.

      Vous pouvez sélectionner la date de début, le fuseau horaire, et l'heure à laquelle la planification doit débuter.
14. Sélectionnez la **Fin de la récurrence** parmi les options suivantes :
    - Pas de date de fin : Sélectionnez cette option sur la sauvegarde doit se faire indéfiniment.
    - Date de fin : Sélectionnez cette option si la planification doit se terminer à une date spécifique. La date de fin se trouve sur le même fuseau que la date de début.

    L'option **Fin de la récurrence** n'est pas disponible si vous avez sélectionné **Une fois**.
15. Spécifiez la **Durée estimée**. Cette valeur détermine l'ordre dans lequel les planifications sont affichées dans la vue Agenda.

    Cliquez sur **Suivant**. La page Résumé s'affiche.
16. Contrôlez toutes les options de planification. Si des conflits de planification apparaissent, l'option **Conflits trouvés** est notée **Oui**, et vous ne pouvez terminer la tâche de création de planification tant que vous n'aurez pas accompli l'une des actions suivantes :
    - Redéfinissez le modèle de récurrence de la planification. Cliquez sur Précédent pour retourner à la page **Récurrence**.

- Mettez l'option **Remplir les tranches horaires libres** sur ON. Cette option n'est disponible que si des tranches horaires libres sont disponibles à la date sélectionnée. S'il n'y a pas de tranche horaire libre, vous devez redéfinir le modèle de récurrence de la planification.

Cliquez sur **Terminer** pour créer la planification.

Modification d'une planification existante

Exécutez les étapes suivantes pour modifier une planification existante.

> **REMARQUE :**
> Si vous modifiez l'une des options suivantes pour une planification, la planification est supprimée, et une nouvelle planification est créée, avec de nouvelles valeurs. La nouvelle planification est déplacée à la fin de la file d'attente, et, selon les disponibilités de tranches horaires, le statut est appliqué.
>
> - Date de lancement
> - Date de fin
> - Fuseau horaire
> - Modèle de récurrence
> - Valeur de chaque nième
> - Durée estimée
> - Jours chômés

Les étapes de cette procédure expliquent comment modifier une planification de spécification de sauvegarde. Les options disponibles dans l'assistant de planification sont basées sur les types de spécifications que vous choisissez.

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**, puis le type de spécification approprié (par exemple **système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Faites un clic droit sur la spécification de sauvegarde appropriée, puis cliquez sur **Modifier planification**. La page du Planificateur s'affiche. Toutes les planifications disponibles pour la spécification de sauvegarde sont visibles dans le panneau de droite.
4. Sur la page du Planificateur, cliquez sur l'icône **Modifier** pour la planification dont vous voulez modifier la configuration. La page Options de l'assistant planification s'ouvre.
5. Mettez à jour le nom de votre planification dans la boîte de texte **Nom de planification**.

   > **IMPORTANT :**
   > Pour les planifications qui ont migré depuis des versions Data Protector antérieures à la version 10.00, le nom de planification apparaît comme **...**.

6. Sélectionnez le type de **Sauvegarde**, Complète ou Incrémentale. Pour plus d'informations sur les différents types d'options de sauvegarde, consultez la section Types de sauvegardes.
7. Sélectionnez le **Niveau de protection**. Le niveau de protection détermine la durée pendant laquelle les informations sur les données sauvegardées sont conservées dans l'IDB. En l'absence

de protection de catalogue, vous pouvez restaurer les données mais pas les parcourir via l'interface Data Protector. Sélectionnez l'une des options suivantes.

- Aucune : Ne définit aucune protection.
- Valeur par défaut : Les informations stockées dans la base de données interne sont protégées contre l'écrasement tant que les données sont protégées.
- Jusqu'au : Les informations de l'IDB ne sont pas écrasées avant la date spécifiée. La protection des données s'arrête le jour indiqué à midi.
- Jours : Les informations de l'IDB ne sont pas écrasées pendant le nombre de jours spécifié.
- Semaines : Les informations de l'IDB ne sont pas écrasées pendant le nombre de semaines spécifié.
- Permanent : Les informations de l'IDB sont disponibles de manière permanente.

8. Déplacez le curseur pour définir la priorité, ou entrez un nombre dans la boîte de texte **Priorité** si le nombre de priorité est supérieur aux valeurs du curseur. Le niveau de priorité est considéré si plusieurs sessions essaient d'accéder à un périphérique au même moment. Dans ce cas, cette option détermine l'ordre dans lequel les sessions seront mises en attente.

   Si une session de priorité inférieure est en cours lorsqu'une session de priorité supérieure est mise en file d'attente, la session en cours est autorisée à se terminer. Lorsque plusieurs sessions avec la même priorité demandent l'accès à un périphérique, chacune de ces sessions peut obtenir l'accès en premier.
9. Spécifiez la **charge réseau**. La définition de cette option sur Moyenne or Bas permet de réduire la charge réseau lorsque vous exécutez Data Protector. Ainsi, le processus de transmission des données ne bloque pas l'accès des autres utilisateurs au réseau, mais le temps d'exécution de la session est plus important.
10. Mettez l'option **Mise en pause des tâches de priorité inférieure** sur ON, si la session planifiée doit être en mesure de pouvoir mettre n pause des sessions de priorité inférieure sur un périphérique occupé. Cette option est utile si plusieurs sessions tentent d'accéder en même temps à un périphérique. Dans ce cas, l'option spécifie que la session sélectionnée peut suspendre d'autres sessions jusqu'à ce qu'elle se termine. Une fois la session terminée, les sessions suspendues reprennent jusqu'à leur terme.

    REMARQUE :
    Cette fonctionnalité est disponible pour les sessions d'intégration de système de fichiers, VMware et Oracle Server. Les sessions de sauvegarde Backup to Disk (B2D) ne peuvent pas être suspendues en fonction d'une priorité. Pour les sessions de sauvegarde contenant une combinaison de types de périphériques de sauvegarde, par exemple une bibliothèque de fichiers et un système B2D, la fonctionnalité de suspension s'applique uniquement aux périphériques non-B2D.
11. La planification est activée par défaut. Pour désactiver la planification, mettez l'option **Planification activée** sur OFF.
12. Mettez l'option **Jours chômés** sur ON si vous souhaitez que les opérations soient lancées également les jours chômés. Par défaut, Data Protector exécute les opérations planifiées les jours chômés également. Pour spécifier différents jours comme jours chômés, modifiez le fichier des

jours chômés.

Cliquez sur **Suivant**. La page Récurrence s'affiche.

13. Sous Modèle de récurrence, indiquez la fréquence des sauvegardes. Sélectionnez le modèle et la fréquence parmi les options suivantes :
    - **Une fois**: La planification s'effectue une seule fois à la date spécifiée. Vous pouvez sélectionner la date de début, le fuseau horaire, et l'heure à laquelle la planification doit débuter.
    - **Quotidienne** : La planification s'effectue régulièrement, à l'heure spécifiée. Vous pouvez spécifier la fréquence de la planification en utilisant le champ Tous les <valeur> Jour(s). Par exemple, une valeur de récurrence de 4 signifie que la planification s'effectuera tous les quatre jours.

      Vous pouvez sélectionner la date de début, le fuseau horaire, et l'heure à laquelle la planification doit débuter.
    - **Hebdomadaire** : La planification s'effectue chaque semaine, le jour spécifié. Vous pouvez spécifier la fréquence de la planification en utilisant le champ Toutes les <valeur> Semaine(s). Par exemple, une valeur de récurrence de 2 signifie que la planification s'effectuera toutes les deux semaines, le jour indiqué.

      Vous pouvez sélectionner la date de début, le fuseau horaire, et l'heure à laquelle la planification doit débuter.
    - **Mensuelle** : La planification s'effectue chaque mois, le jour spécifié. Vous pouvez spécifier la fréquence de la planification en utilisant le champ Tous les <valeur> Mois. Par exemple, une valeur de 2 signifie que la planification s'effectuera tous les deux mois, le jour indiqué.

      Vous pouvez sélectionner la date de début, le fuseau horaire, et l'heure à laquelle la planification doit débuter.
14. Sélectionnez la **Fin de la récurrence** parmi les options suivantes :
    - Pas de date de fin : Sélectionnez cette option sur la sauvegarde doit se faire indéfiniment.
    - Date de fin : Sélectionnez cette option si la planification doit se terminer à une date spécifique. La date de fin se trouve sur le même fuseau que la date de début.

    L'option **Fin de la récurrence** n'est pas disponible si vous avez sélectionné **Une fois**.
15. Spécifiez la **Durée estimée**. Cette valeur détermine l'ordre dans lequel les planifications sont affichées dans la vue Agenda.

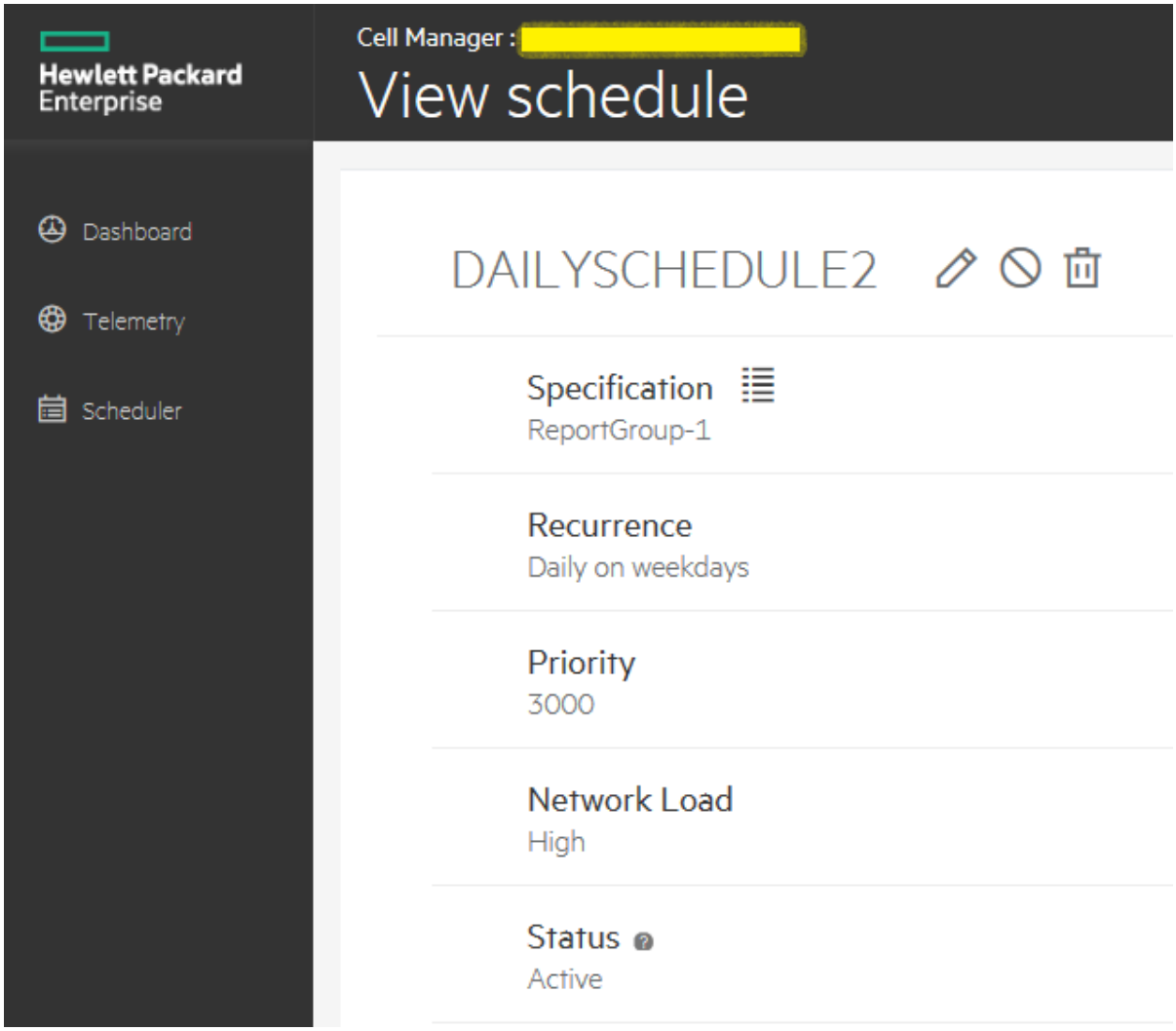
    Cliquez sur **Suivant**. La page Résumé s'affiche.
16. Contrôlez toutes les options de planification. Si des conflits de planification apparaissent, l'option **Conflits trouvés** est notée **Oui**, et vous ne pouvez terminer la tâche de création de planification tant que vous n'aurez pas accompli l'une des actions suivantes :
    - Redéfinissez le modèle de récurrence de la planification. Cliquez sur Précédent pour retourner à la page **Récurrence**.
    - Mettez l'option **Remplir les tranches horaires libres** sur ON. Cette option n'est disponible que si des tranches horaires libres sont disponibles à la date sélectionnée. S'il n'y a pas de tranche horaire libre, vous devez redéfinir le modèle de récurrence de la planification.

Cliquez sur **Terminer** pour enregistrer la planification.

Visualiser une planification

Pour visualiser les détails d'une planification particulière, cliquez sur le nom de la planification dans la vue de l'agenda.

Pour visualiser toutes les planifications de cette spécification, cliquez sur l'icône sur la page Affichage de la planification. Toutes les planifications disponibles pour cette spécification sont visibles dans le panneau de droite.



La page d'Affichage de la planification montre les détails suivants concernant la planification :

- Spécification : le type de spécification pour lequel la planification a été créée.
- Récurrence : le modèle de récurrence paramétré pour la planification.
- Priorité : la priorité de planification qui détermine l'ordre dans lequel la planification sera exécutée.
- Charge réseau : les valeurs actuelles paramétrées pour la charge du réseau lors de l'exécution de Data Protector.

- État : le paramètre d'état montre les valeurs suivantes, selon la disponibilité des tranches horaires :
  - Active : la planification n'a pas de conflit, et s'exécutera à l'heure planifiée.
  - Chevauchement : la planification est en état de conflit, mais des tranches horaires sont encore disponibles le jour sélectionné, où la planification peut s'exécuter.
  - Inactive : la planification est en état de conflit, et aucune tranche horaire n'est plus disponible le jour sélectionné, où la planification peut s'exécuter.
  - Désactivée : la planification a été explicitement désactivée par l'utilisateur.

Désactivation et activation d'une planification

Par défaut, la planification est activée lorsqu'elle est ajoutée, mais vous pouvez la désactiver en laissant intacts les paramètres de planification pour une utilisation ultérieure.

La désactivation des planifications de sauvegarde n'influe pas sur l'exécution des sessions de sauvegarde en cours.

Les étapes de cette procédure expliquent comment désactiver et activer une planification de spécification de sauvegarde. Les options disponibles dans l'assistant de planification sont basées sur les types de spécifications que vous choisissez.

Procédure

1. Dans la liste de contexte, sélectionnez **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis le type de spécification approprié (par exemple, **Système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Faites un clic droit sur la spécification de sauvegarde appropriée, puis cliquez sur **Modifier planification**. La page Vue planification s’affiche. Toutes les planifications disponibles pour la spécification de sauvegarde sont visibles dans le panneau de droite.
4. Cliquez sur la planification que vous souhaitez modifier, puis cliquez sur l'icône **Modifier planification** sur la page Vue planification. L'assistant planification s’ouvre.
5. Dans la page Options, mettez le curseur de **Planification activée** sur **OFF** pour désactiver la planification, puis cliquez sur **Suivant**. Mettez le curseur sur **ON** pour activer la planification. La page Récurrence s’affiche.
6. Vérifiez le modèle de récurrence, puis cliquez sur **Suivant**. La page Résumé s’affiche.
7. Vérifiez les options de planification, puis cliquez sur **Terminer**.

Désactiver et activer une planification les jours chômés

Par défaut, Data Protector exécute les planifications les jours chômés. Toutefois, vous pouvez modifier ce comportement en sélectionnant l'option **Jours chômés**. Ainsi, les sauvegardes ne s'effectuent pas les jours chômés tant que vous ne désélectionnez pas cette option.

Les étapes de cette procédure expliquent comment activer et désactiver une planification de spécification de sauvegarde. Les options disponibles dans l'assistant de planification sont basées sur les types de spécifications que vous choisissez.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécifications de sauvegarde**, puis le type de spécification de sauvegarde (par exemple **Système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Faites un clic droit sur la spécification de sauvegarde dont vous souhaitez activer ou désactiver la planification pendant les jours chômés, puis cliquez sur **Modifier planification**. La page du Planificateur s'affiche. Toutes les planifications disponibles pour la spécification de sauvegarde sont visibles dans le panneau de droite.
4. Cliquez sur la planification que vous souhaitez modifier, puis cliquez sur l'icône **Modifier planification** sur la page Vue planification. L'assistant planification s'ouvre.
5. Dans la page Otions, mettez le curseur **Jours chômés sur OFF** pour éviter que l'opération soit effectuée les jours chômés. Mettez le curseur sur **ON** si vous voulez que l'opération soit effectuée les jours chômés.
6. Cliquez sur **Suivant**. La page Récurrence s'affiche.
7. Vérifiez le modèle de récurrence, puis cliquez sur **Suivant**. La page Résumé s'affiche.
8. Vérifiez les options de planification, puis cliquez sur **Terminer**.

Définition d'une planification à une date et une heure spécifiques

Vous pouvez planifier vos sessions afin qu'elles démarrent automatiquement à une date et une heure données.

Les étapes de cette procédure expliquent comment configurer une planification de spécification de sauvegarde à une date et une heure précises. Les options disponibles dans l'assistant de planification sont basées sur les types de spécifications que vous choisissez.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**, puis le type de spécification approprié (par exemple **système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Faites un clic droit sur la spécification de sauvegarde appropriée, puis cliquez sur **Modifier planification**. La page de planification s'affiche. Toutes les planifications disponibles pour la spécification de sauvegarde sont visibles dans le panneau de droite.
4. Cliquez sur la planification que vous souhaitez modifier, puis cliquez sur l'icône **Modifier planification**. L'assistant planification s'ouvre.
5. Contrôlez les paramètres dans la page Options, et cliquez sur **Suivant**. La page Récurrence s'affiche.
6. Sous Modèle de récurrence, sélectionnez **Une fois**, puis spécifiez la date de début, le fuseau

horaire et l'heure de début de la sauvegarde. Vous pouvez également spécifier la durée de la sauvegarde, et cliquer sur **Suivant**.

7. Contrôlez les options de la planification dans la page Résumé, et cliquez sur **Terminer**.

Si vous planifiez une sauvegarde dans une tranche horaire qui est déjà occupée par une autre sauvegarde, la nouvelle sauvegarde planifiée remplace la précédente.

Planifier une sauvegarde périodique

Une planification périodique est une planification qui s'exécute à intervalles réguliers. Par exemple, vous pouvez configurer des sauvegardes périodiques de sorte qu'une sauvegarde complète ait lieu le dimanche à 03h00 puis tous les deux jours. La prochaine sauvegarde complète interviendra à 03h00 le mardi suivant. Les sauvegardes périodiques simplifient la configuration des sauvegardes régulièrement planifiées.

Vous pouvez planifier une sauvegarde périodique pendant que vous créez un nouveau type de spécification à l'aide de l'assistant, ou vous pouvez modifier la planification d'une spécification existante, comme décrit dans les procédures suivantes.

Les étapes de cette procédure indiquent comment planifier une spécification de sauvegarde périodique. Les options disponibles dans l'assistant de planification sont basées sur les types de spécifications que vous choisissez.

Utilisation d'une planification de sauvegarde prédéfinie

Les planifications de sauvegarde prédéfinies peuvent être utilisées pour simplifier la configuration de sauvegarde d'un système de fichiers. Vous pouvez modifier les planifications ultérieurement.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis **Système de fichiers**. Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Faites un clic droit sur la spécification de sauvegarde appropriée, puis cliquez sur **Modifier planification**. L'assistant planification s’ouvre.
4. Dans la page Type, sélectionnez **Prédéfini**, puis sélectionnez une planification appropriée dans la liste des Planifications prédéfinies. Sélectionnez l'une des propositions suivantes :
   - Intensive - Quotidienne : Data Protector lance une sauvegarde complète à minuit et deux sauvegardes incrémentales à 12h00 (midi) et 18h00 (6 pm) chaque jour.
   - Complète - Quotidienne : Data Protector lance une sauvegarde complète chaque jour à 21h00 (9 pm).
   - Complète - Hebdomadaire : Data Protector lance une sauvegarde complète chaque vendredi et des sauvegardes Incr1 chaque jour du lundi au vendredi à 21h00 (9 pm).

- Complète - Tous les 15 jours : Data Protector lance une sauvegarde complète un vendredi sur deux. Entre ces sauvegardes, Data Protector lance des sauvegardes Incr1 tous les jours, du lundi au jeudi, à 21h00 (9 pm).
- Complète - Mensuelle : Data Protector lance une sauvegarde complète tous les mois, une sauvegarde Incr1 toutes les semaines, et une sauvegarde incrémentale un jour sur deux.

Cliquez sur **Suivant**. La page Options s'affiche.

5. Spécifiez les options dans la page Options, et cliquez sur **Suivant**. La page Récurrence s'affiche.
6. Spécifiez les options dans la page Récurrence, et cliquez sur **Suivant**. La page Résumé s'affiche.
7. Vérifiez les options de planification, puis cliquez sur **Terminer**.

Configuration d'une planification périodique

Vous pouvez créer une planification de façon à ce qu'elle commence à une date et une heure précises, et se répète selon un modèle défini. Par exemple, vous pouvez planifier une sauvegarde complète afin qu'elle ait lieu tous les vendredis à 21h00 au cours des six prochains mois.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis le type de spécification approprié (par exemple, **Système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Faites un clic droit sur la spécification de sauvegarde appropriée, puis cliquez sur **Modifier planification**. L'assistant planification s'ouvre.
4. Dans la page Type, sélectionnez **Personnalisé** et cliquez sur **Suivant**. La page Options s'affiche.
5. Dans la zone de texte Nom de planification, entrez un nom pour la nouvelle planification. Sélectionnez un type de sauvegarde (complète ou incrémentale ; d'autres types de sauvegarde sont disponibles pour certaines intégrations, protection de sauvegarde, priorité, et charge réseau). Cliquez sur **Suivant**. La page Récurrence s'affiche.
6. Sous Modèle de récurrence, sélectionnez le modèle et la fréquence parmi les options suivantes :
   - **Quotidienne** : la planification s'effectue régulièrement, à l'heure spécifiée. Vous pouvez spécifier la fréquence de la planification en utilisant le champ Tous les <valeur> Jour(s). Par exemple, une valeur de récurrence de 4 signifie que la planification s'effectuera tous les quatre jours.
   - **Hebdomadaire** : la planification s'effectue chaque semaine, le jour spécifié. Vous pouvez spécifier la fréquence de la planification en utilisant le champ Toutes les <valeur> Semaine(s). Par exemple, une valeur de récurrence de 2 signifie que la planification s'effectuera toutes les deux semaines, le jour indiqué.
   - **Mensuelle** : la planification s'effectue chaque mois, le jour spécifié. Vous pouvez spécifier la fréquence de la planification en utilisant le champ Tous les <valeur> Mois. Par exemple, une valeur de 2 signifie que la planification s'effectuera tous les deux mois, le jour indiqué.

7. Spécifiez la plage de récurrence parmi les options suivantes, puis cliquez sur **Suivant**.
   - Début : la date initiale de la planification. Spécifiez la date, le fuseau horaire et l'heure de début de la planification.
   - Fin de récurrence : la date à laquelle la dernière planification doit s'exécuter. Sélectionner **Pas de date de fin** sir la planification doit s'exécuter indéfiniment.

   > **REMARQUE :**
   > Si vous définissez la périodicité sur 2 ou plus (par exemple, toutes les deux semaines le samedi) sans définir la date de début, la première session de sauvegarde peut ne pas être planifiée à la première date possible qui correspond à votre sélection (par exemple, elle sera planifiée le deuxième samedi) en raison de l'algorithme de planification de Data Protector.
8. Contrôlez les options de la planification dans la page Résumé, et cliquez sur **Terminer**.
9. Dans le cas de ZDB sur disque + bande ou ZDB sur disque (la restauration instantanée est activée), spécifiez l'option Sauvegarde Split Mirror/Snapshot.

   Cliquez sur **OK**.

Data Protector vous informe en cas de conflits de planification afin que vous puissiez modifier la planification.

Conseils de planification

Suivez les conseils ci-après lors de la création de planifications :

- Lorsqu'une planification démarre, Data Protector tente d'allouer toutes les ressources nécessaires, telles que les licences, les périphériques et l'accès à l'IDB. Si l'une des ressources nécessaires n'est pas disponible, la session est mise en attente pendant que Data Protector tente d'obtenir les ressources nécessaires à la session mise en attente toutes les minutes jusqu'à ce que le délai d'expiration soit atteint. Le délai d'expiration peut être modifié en changeant l'option globale `SmWaitForDevice`.

  Lorsque Data Protector obtient les ressources, les sessions en attente sont démarrées. Les sessions en attente risquent de ne pas démarrer dans l'ordre où elles s'affichent.
- Pour empêcher toute surcharge de Gestionnaire de cellule, le nombre de sessions simultanées dans une cellule est limité par défaut. Si le nombre de sessions simultanées prévues dépasse la limite effective, et que cette limite effective est inférieure à la limite maximale configurable, les sessions en trop sont mises en attente. La limite peut être modifiée à l'aide de l'option globale `MaxBSessions`.

  En revanche, les sessions simultanément invoquées qui dépassent la limite maximale configurable ne sont pas démarrées, et les erreurs correspondantes sont enregistrées dans le Journal d'événements Data Protector.
- Pour simplifier la planification, Data Protector fournit des spécifications de sauvegarde pour les clients d'un groupe. Tous les clients configurés dans une spécification de sauvegarde sont sauvegardés en même temps dans une seule session de sauvegarde.
- Assurez-vous que vous avez suffisamment de supports et de périphériques pour exécuter facilement des sauvegardes sans surveillance.
- Lorsque vous appliquez un modèle de sauvegarde, les paramètres de planification de ce modèle

remplacent ceux de la spécification de sauvegarde. Après avoir appliqué le modèle, vous pouvez toujours modifier la spécification de sauvegarde et définir une autre planification.

- La granularité du planificateur est définie par le modèle de récurrence et représente au moins 1 minute.
- Lorsque les sessions de sauvegarde et de copie sont lancées, elles nécessitent d'affecter de la mémoire car elles consomment beaucoup de ressources, en particulier sur les serveurs d'Agent de support. Vous devez donc vous assurez que plusieurs sessions de sauvegarde et de copie ne démarrent pas en même temps. Par exemple, si vous devez lancer neuf spécifications de sauvegarde aux environs de 18h00, vous devez commencer les trois premières sauvegardes à 17h45, les trois suivantes à 18h00, puis les trois dernières à 18h15, au lieu de planifier les neuf sauvegardes pour qu'elles commencent à 18h00.

Chapitre 8: Périphériques

À propos des périphériques de sauvegarde

Data Protector définit et élabore un périphérique physique avec les propriétés d'utilisation de Data Protector. Il est possible d'avoir plusieurs définitions Data Protector pour un même périphérique physique. Ce concept de périphérique vous permet de configurer des périphériques de manière aisée et flexible et de les utiliser dans la spécification de sauvegarde.

Qu'est-ce qu'un périphérique de sauvegarde ?

Périphérique physique configuré pour une utilisation avec Data Protector, capable d'écrire et de lire des données sur des supports de stockage. Il peut s'agir, par exemple, d'un lecteur DDS/DAT autonome ou d'une bibliothèque.

Pour obtenir une liste des périphériques pris en charge par Data Protector, reportez-vous à la matrice de prise en charge de périphériques HPE Data Protector Les périphériques non pris en charge peuvent être configurés à l'aide du fichier `scsitab`.

Certains périphériques de sauvegarde (par exemple, lecteurs de bandes) font l'objet de licences Data Protector particulières. Consultez le *Guide d'installation HPE Data Protector* pour plus de détails.

A propos de la configuration des périphériques de sauvegarde

Une fois la phase de préparation terminée, vous pouvez configurer un périphérique de sauvegarde à utiliser avec Data Protector.

Il est recommandé de laisser Data Protector configurer automatiquement les périphériques de sauvegarde. Data Protector peut automatiquement configurer les périphériques de sauvegarde les plus courants, notamment les bibliothèques. Vous devez toujours préparer le support pour une session de sauvegarde, mais Data Protector détermine le nom, la stratégie, le type de support, la stratégie de support et le fichier de périphérique ou l'adresse SCSI du périphérique, et configure le lecteur et les emplacements.

Vous pouvez également configurer manuellement un périphérique de sauvegarde. La configuration d'un périphérique de sauvegarde dépend de son type.

Vous pouvez utiliser des périphériques qui ne sont pas mentionnés comme étant pris en charge dans *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*. Les périphériques non pris en charge sont configurés à l'aide du fichier `scsitab`.

> **REMARQUE :** Le contrôle externe est un moyen de contrôler les bibliothèques inconnues de Data Protector. Si Data Protector ne prend pas en charge un périphérique particulier, un utilisateur peut écrire un script ou un programme qui exécutera la fonction de contrôle robotique afin de charger un support sur le lecteur indiqué depuis un emplacement donné. Il est possible de configurer une bibliothèque comme contrôle externe en se référant à un script spécial.

Types de périphériques de sauvegarde

Data Protector Data Protector prend en charge les types de périphériques suivants, que vous pouvez configurer (selon les composants que vous avez installés) :

- Autonome
- Périphérique de sauvegarde sur disque
- Bibliothèque SCSI
- Chargeur
- Périphérique de magasin
- Bibliothèque de bandes magnéto-optiques
- Périphérique de fichier autonome
- Périphérique de bibliothèque de fichiers
- Contrôle externe
- Bibliothèque DAS ADIC/GRAU
- Bibliothèque ACS StorageTek

Autonome

Un périphérique autonome est un simple périphérique comportant un lecteur qui lit ou écrit sur un support à la fois, DDS ou DLT par exemple. Ces périphériques sont utilisés pour les sauvegardes à petite échelle. Dès que le support est plein, un opérateur doit le remplacer manuellement par un nouveau support afin de poursuivre la sauvegarde. Les périphériques autonomes ne conviennent donc pas pour les grandes sauvegardes sans surveillance.

Périphérique de sauvegarde sur disque

Un périphérique de sauvegarde sur disque (B2D) est un périphérique de stockage sur disque qui offre des fonctionnalités supplémentaires par rapport à une bibliothèque de bandes magnéto-optiques Data Protector ou à un périphérique de bibliothèque de fichiers, comme l'accès via des hôtes multiples (*passerelles*) ou, en fonction du type du périphérique, la déduplication.

Bibliothèque SCSI

Les périphériques de bibliothèque SCSI sont des périphériques de sauvegarde grande capacité, également appelés chargeurs automatiques. Ils se composent d'un certain nombre de cartouches de support installées dans le référentiel d'un périphérique, et peuvent comporter plusieurs lecteurs gérant plusieurs supports à la fois. La plupart des périphériques de bibliothèque intègrent également un système de nettoyage automatique lorsque le lecteur est sale.

Un périphérique de bibliothèque standard possède un ID SCSI (systèmes Windows) ou un fichier de périphérique (systèmes UNIX) pour chaque lecteur, et un pour le mécanisme robotique de la bibliothèque, qui déplace les supports entre les emplacements et les lecteurs dans un mouvement de

va-et-vient. (Par exemple, une bibliothèque avec quatre lecteurs possède cinq ID SCSI, quatre pour les lecteurs et un pour le mécanisme robotique).

Un support est stocké dans un emplacement du référentiel du périphérique. Data Protector attribue un numéro à chaque emplacement, en commençant par 1. Lors de la gestion d'une bibliothèque, vous vous référez aux emplacements en utilisant leurs numéros.

L'index du lecteur identifie la position mécanique du lecteur dans la bibliothèque. Le numéro d'index est utile pour le contrôle du robot. Le robot de la bibliothèque ne connaît que le numéro d'index du lecteur et n'a aucune information sur son adresse SCSI. L'index du lecteur est un entier séquentiel (commençant à 1) qui doit être couplé avec l'adresse SCSI du lecteur. De nombreuses interfaces Web vers une bibliothèque SCSI, CommandView TL ou panneau de commande de bibliothèque SCSI numérotent les lecteurs à partir de '0'. Un lecteur '0' est pas valide dans la configuration des périphériques Data Protector : le premier lecteur doit toujours être '1'.

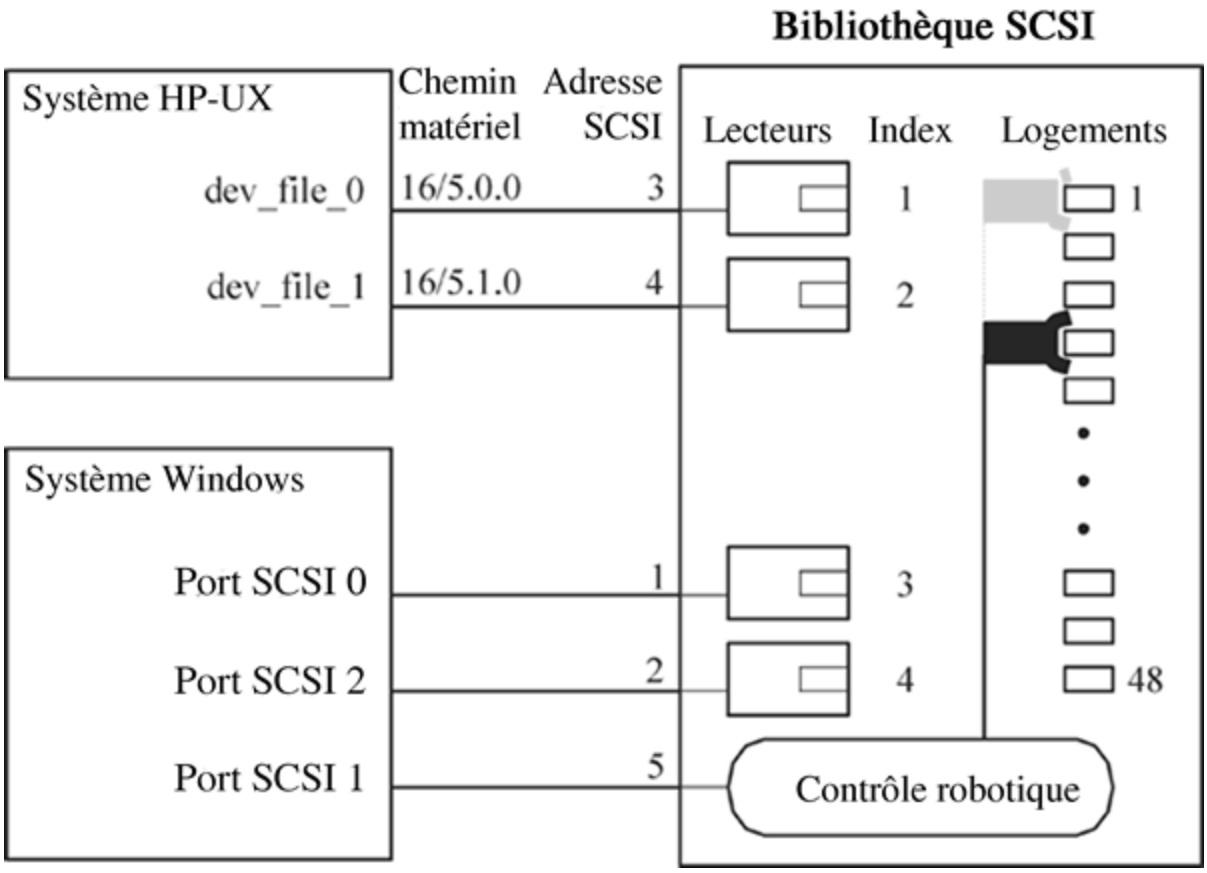
Par exemple, pour une bibliothèque de quatre lecteurs, les index des lecteurs sont 1, 2, 3 et 4. Si la bibliothèque ne contient qu'un seul lecteur, l'index de ce lecteur est 1.

L'index du lecteur doit correspondre à l'adresse SCSI. Cela signifie que vous devez configurer les paires :

Adresse SCISI_A pour l'index 1, Adresse SCISI_B pour l'index 2, et ainsi de suite.

Spécifiez ce type de périphérique également lors de la configuration d'un périphérique de magasin.

Mappage de l'index de lecteur à l'adresse SCSI



Chargeur

Un chargeur est un périphérique unique comportant généralement un seul lecteur. Il charge les supports selon un ordre séquentiel et non aléatoire. Pour cette raison, une stratégie d'allocation de supports Souple est recommandée. Un chargeur prend un support à partir d'une "pile" (son référentiel) et l'insère dans le lecteur. Cet échange se limite toujours à l'éjection du support déjà dans le lecteur et à l'insertion du prochain support de la pile. La charge s'effectue automatiquement, à l'exception du premier support, qui doit être chargé manuellement. Quand une bande est pleine, elle est éjectée puis la bande suivante est automatiquement chargée. Lorsque toutes les bandes sont utilisées dans un magasin de chargeur, le magasin doit être démonté manuellement et le magasin suivant doit être inséré. Ici encore, la première bande doit être chargée manuellement dans le lecteur.

Une session de sauvegarde ou de restauration ne sera pas abandonnée si des médias ne sont pas présents, mais une demande de montage sera soumise à la place. La session complète ne sera pas abandonnée si vous ne changez pas les magasins du chargeur dans un certain délai.

Périphérique de magasin

Un périphérique de magasin regroupe un certain nombre de supports dans une même unité appelé magasin. Un magasin vous permet de gérer de grandes quantités de données plus facilement qu'en utilisant de nombreux supports individuels. Les opérations sur chaque support dans le magasin sont intégralement contrôlées par Data Protector. Le système HPE XP DAT 24x6 peut être configuré comme un périphérique de magasin.

Bibliothèque de bandes magnéto-optiques

Une bibliothèque de bandes magnéto-optiques est un périphérique de bibliothèque qui peut contenir des supports optiques ou des fichiers. Si les supports sont des fichiers, elle est appelée "périphérique de bibliothèque de stockage de fichiers". Le type de support sur le périphérique est défini lors de la configuration initiale.

Si vous utilisez une bibliothèque de bandes-optique sous UNIX, vous devez configurer un fichier de périphérique UNIX pour chaque emplacement de l'échangeur ou face du disque.

Périphérique de fichier autonome

Un périphérique de fichier autonome est un fichier résidant dans un répertoire déterminé, dans lequel vous sauvegardez des données au lieu de les écrire sur une bande.

Périphérique de bibliothèque de fichiers

Un périphérique de bibliothèque de fichiers est un ensemble de répertoires dans lequel vous sauvegardez des données au lieu de les écrire sur une bande.

Contrôle externe

Le contrôle externe est un moyen de contrôler les bibliothèques inconnues de Data Protector. Si Data Protector ne prend pas en charge un périphérique particulier, un utilisateur peut écrire un script ou un programme qui exécutera la fonction de contrôle robotique afin de charger un support sur le lecteur indiqué depuis un emplacement donné. Il est possible de configurer une bibliothèque comme contrôle externe en se référant à un script spécial.

Bibliothèque DAS ADIC/GRAU

Une bibliothèque DAS ADIC/GRAU est une très grande bibliothèque contrôlée (silo). Elle est utilisée dans des environnements complexes où la quantité de données sauvegardées est exceptionnellement élevée, comme par conséquent la quantité de supports nécessaires pour stocker ces données. Elle peut gérer d'une centaine à plusieurs milliers de bandes. Généralement, une bibliothèque DAS ADIC/GRAU peut accueillir de nombreux types de lecteurs de sauvegarde et des milliers d'emplacements de supports, tous desservis par un mécanisme robotique interne, et contrôlés par des unités de contrôle de bibliothèque spéciales. Vous pouvez affecter un ensemble dédié de supports de la bibliothèque à une application afin de partager cette bibliothèque entre Data Protector et d'autres applications.

Toutes les opérations sur les supports peuvent être exécutées à partir de l'interface utilisateur de Data Protector. Pour les supports dont le format est reconnu, Data Protector affiche le format sous forme de type de support, `tar` par exemple. Pour les supports dont le format n'est pas reconnu, le type de support est `foreign`.

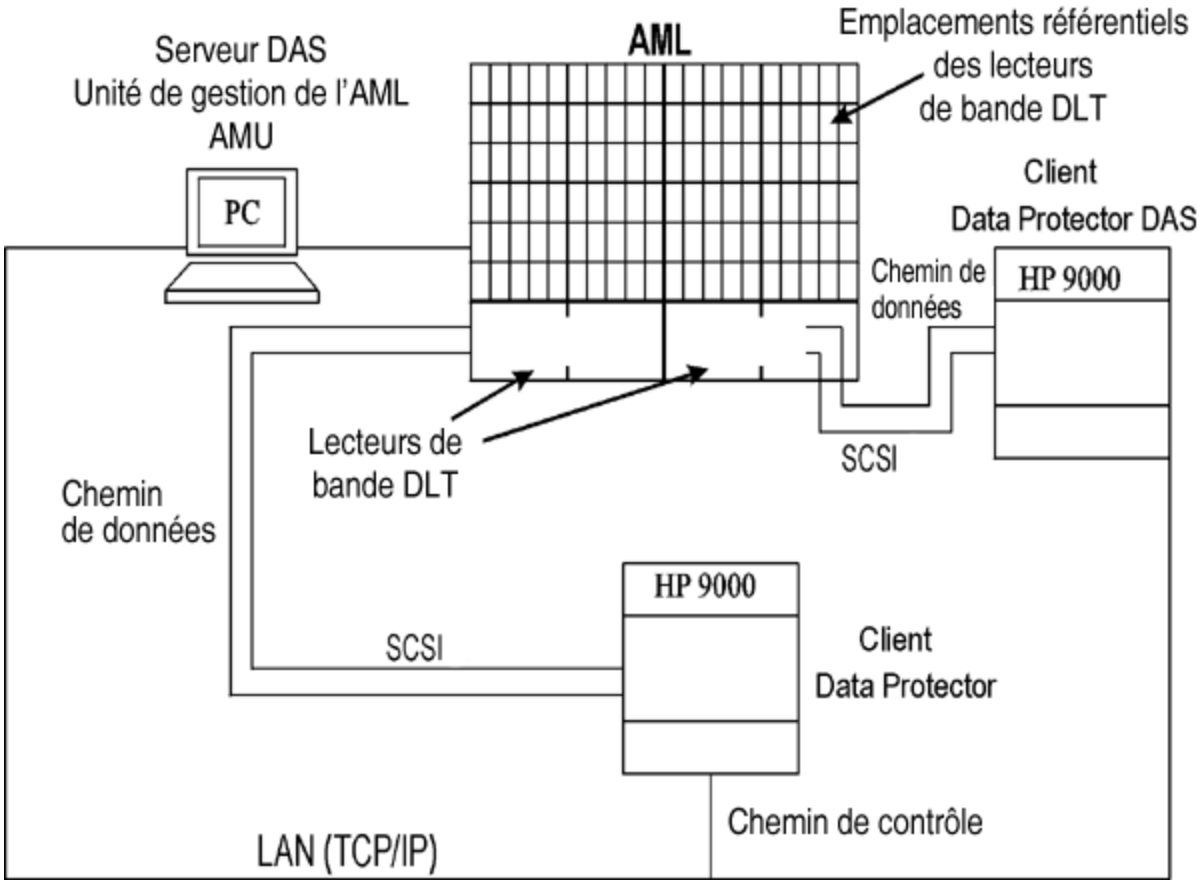
La base de données de gestion des supports analyse tous les supports Data Protector et non-Data Protector, qu'ils soient résidents (supports dans le référentiel du périphérique) ou non-résidents (supports à l'extérieur du référentiel du périphérique), offrant ainsi une protection sophistiquée contre l'écrasement de données. Data Protector n'écrasera aucun support contenant des données dans un format reconnu. Cependant, il n'est pas garanti que les données Data Protector sur bandes ne seront pas écrasées par une autre application utilisant le même support. Il est recommandé que les supports utilisés par Data Protector ne soient pas utilisés par une autre application, et réciproquement.

L'emplacement réel d'un support est géré par le serveur DAS, qui suit l'emplacement en utilisant son volser. Un support déplacé dans le référentiel n'est pas affecté à chaque fois au même emplacement physique. Par conséquent, vous ne devez pas vous appuyer sur le numéro de l'emplacement lorsque vous gérez des supports, mais sur le code-barres (volser).

La bibliothèque DAS ADIC/GRAU peut automatiquement nettoyer ses lecteurs lorsque le disque a été utilisé un certain nombre de fois. Cette opération n'est cependant pas recommandée car le nettoyage du lecteur interrompt et fait échouer la session en cours. Si vous souhaitez utiliser la fonctionnalité de nettoyage de la bibliothèque, vous devez vous assurer que le nettoyage du lecteur est effectué quand aucune session Data Protector n'est en cours d'exécution.

> **IMPORTANT :**
> Vous devez créer une bibliothèque logique Data Protector pour chaque type de support. Alors que le système ADIC/GRAU ou ACS STK peut stocker de nombreux types de supports physiquement différents, Data Protector peut seulement reconnaître une bibliothèque contenant un seul type de support.

Intégration des systèmes de bibliothèque Data Protector et DAS ADIC/GRAU



Bibliothèque ACS StorageTek

Une bibliothèque Automated Cartridge (ACS) StorageTek est une bibliothèque robotique (silo). Elle est utilisée dans des environnements complexes où la quantité de données sauvegardées est exceptionnellement élevée, comme par conséquent la quantité de supports nécessaires pour stocker ces données. Elle peut gérer des centaines de bandes. Vous pouvez affecter un ensemble dédié de supports du périphérique à une application afin de partager la bibliothèque entre Data Protector et d'autres applications.

Généralement, un tel périphérique comporte de nombreux types de lecteurs de sauvegarde et des milliers d'emplacements de supports, tous desservis par un mécanisme robotique interne, et contrôlés via un logiciel ACS Library Server (ACSLS). Les actions liées aux supports et aux périphériques initiées par Data Protector transitent de l'interface utilisateur vers l'ACSLS, qui contrôle ensuite directement le robot, puis déplace et charge les supports.

Lorsque la bibliothèque est correctement installée et configurée, Data Protector permet de facilement gérer les supports pendant une session de sauvegarde et de restauration. Toutes les opérations sur les supports peuvent être exécutées à partir de l'interface utilisateur de Data Protector. Pour les supports dont le format est reconnu, Data Protector affiche le format sous forme de type de support, `tar` par exemple. Pour les supports dont le format n'est pas reconnu, le type de support est `foreign`.

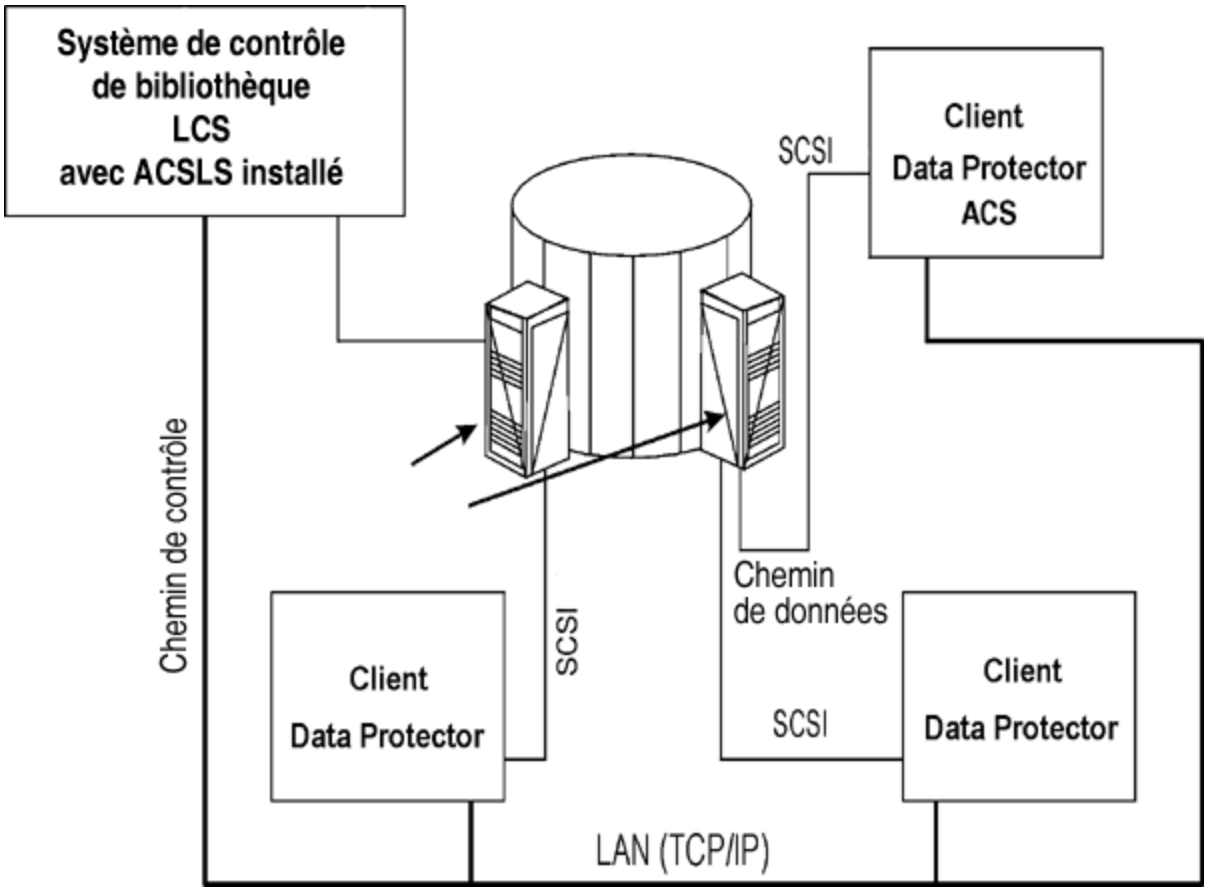
La base de données de gestion des supports analyse tous les supports Data Protector et non-Data Protector, qu'ils soient résidents (supports dans le référentiel du périphérique) ou non-résidents (supports à l'extérieur du référentiel du périphérique), offrant ainsi une protection sophistiquée contre l'écrasement de données. Data Protector n'écrasera aucun support contenant des données dans un format reconnu. Cependant, il n'est pas garanti que les données Data Protector sur bandes ne seront pas écrasées par une autre application utilisant le même support. Il est recommandé que les supports utilisés par Data Protector ne soient pas utilisés par une autre application, et réciproquement.

L'emplacement réel d'un support est géré par le serveur ACS, qui suit l'emplacement en utilisant son volser. Un support déplacé dans le référentiel n'est pas affecté à chaque fois au même emplacement physique. Par conséquent, vous ne devez pas vous appuyer sur le numéro de l'emplacement lorsque vous gérez des supports, mais sur le code-barres (volser).

La bibliothèque ACS StorageTek peut automatiquement nettoyer ses lecteurs lorsque le disque a été utilisé un certain nombre de fois. Cette opération n'est cependant pas recommandée car le nettoyage du lecteur interrompt et fait échouer la session en cours. Si vous souhaitez utiliser la fonctionnalité de nettoyage de la bibliothèque, vous devez vous assurer que le nettoyage du lecteur est effectué quand aucune session Data Protector n'est en cours d'exécution.

> **IMPORTANT :**
> Vous devez créer une bibliothèque logique Data Protector pour chaque type de support. Alors que le système ADIC/GRAU ou ACS STK peut stocker de nombreux types de supports physiquement différents, Data Protector peut seulement reconnaître une bibliothèque contenant un seul type de support.

Intégration de Data Protector et d'une bibliothèque ACS StorageTek



À propos du composant de déduplication du logiciel StoreOnce.

Installation

Cette section propose une présentation des tâches principales et conditions préalables nécessaires pour l'installation du composant de déduplication du logiciel StoreOnce.

Conditions préalables

Vérifiez que le Gestionnaire de cellule, le client d'interface utilisateur, et le serveur d'installation HPE Data Protector 10.00 sont installés sur des systèmes pris en charge.

Pour plus de détails, consultez les dernières matrices de prise en charge HPE Data Protector sur http://support.openview.hp.com/selfsolve/manuals. Consultez le *Guide d'installation et de choix des licences HPE Data Protector* pour des instructions d'installation de Data Protector sur diverses architectures.

Configuration du pare-feu

Vérifiez que les ports suivants sont ouverts aux connexions entrantes :

- `9387/tcp` – port de commande (pour systèmes de logiciel StoreOnce et systèmes de sauvegarde StoreOnce).
- `9388/tcp` – port de données (pour systèmes de logiciel StoreOnce et systèmes de sauvegarde StoreOnce).

Les ports 9387 et 9388 doivent être ouverts dans un pare-feu séparant le périphérique source de toute passerelle. (Systèmes Windows : les ports sont ouverts au cours du processus d'installation, systèmes UNIX : les ports doivent être ouverts manuellement.) Pour plus de détails sur les ports Data Protector, consultez l'index Aide de Data Protector : "plage de ports".

Procédure d'installation

Installez l'Agent de support Data Protector ou le composant d'Agent de support NDMP sur tous les systèmes qui deviendront des passerelles, y compris les clients sur lesquels la déduplication côté source sera activée.

Pour des instructions détaillées, consultez le Guide d'installation HP Data Protector. Pour obtenir une liste détaillée des versions de systèmes d'exploitation pris en charge, consultez les dernières matrices de prise en charge sur http://support.openview.hp.com/selfsolve/manuals.

Opérations supplémentaires pour la déduplication du logiciel StoreOnce

Installez le composant de déduplication du logiciel StoreOnce sur le système voué à héberger la banque StoreOnce.

Le composant de déduplication du logiciel StoreOnce peut être installé en local ou à distance.

Installation à distance du composant de déduplication du logiciel StoreOnce Data Protector

1. Connectez-vous à n'importe quel client doté du composant d'interface utilisateur Data Protector.
2. Ouvrez l'interface utilisateur graphique Data Protector, et, dans la Liste Contexte, sélectionnez les clients.
3. Ajoutez le composant de déduplication du logiciel StoreOnce Data Protector au client de sauvegarde :
   - Si le client de sauvegarde ne fait pas partie de la cellule Data Protector, utilisez la fonctionnalité Data Protector Ajouter clients.
   - Si le client de sauvegarde fait déjà partie de la cellule Data Protector, utilisez la fonctionnalité Data Protector Ajouter composants.

Suite à une installation réussie, le composant de déduplication du logiciel StoreOnce est présent dans la liste Composants installés.

Avant de pouvoir utiliser la déduplication du logiciel StoreOnce, le répertoire source des banques doit être configuré.

Installation en local du composant de déduplication du logiciel StoreOnce Data Protector

Systèmes Windows :
Pendant une installation en local de Data Protector, sélectionnez le composant `the StoreOnce Software Deduplication` dans la liste Composants.

Systèmes Linux :
Exécutez `omnisetup.sh -installStoreOnceSoftware`.

Configurer le service/démon StoreOnceSoftware

Systèmes Windows :
Suite à une installation réussie, l'exécutable StoreOnceSoftware est lancé en tant que service (consultez l'onglet Services dans le Gestionnaire de tâches). Le nom de service est Data Protector StoreOnceSoftware, la description est `StoreOnce Software Deduplication`, et le type de démarrage est automatique.

Systèmes Linux :
Pour installer le démon StoreOnceSoftware de façon à ce qu'il démarre automatiquement après un redémarrage du système, copiez le fichier `StoreOnceSoftwared` dans le répertoire `/etc/init.d` et incluez-le dans les scripts de démarrage. Le démon peut également être démarré ou arrêté manuellement à l'aide des commandes :

```
/opt/omni/lbin/StoreOnceSoftwared start
```

et

```
/opt/omni/lbin/StoreOnceSoftwared stop
```

La suppression du composant de déduplication du logiciel StoreOnce du système arrête automatiquement le processus et supprime le fichier `StoreOnceSoftwared` du répertoire `/etc/init.d/`.

Structure du répertoire installé

Systèmes Windows :
Le composant d'installation comprend les fichiers suivants :

Nom de fichier	Emplacement du fichier
`StoreOnceSoftware.exe`	*`Data_Protector_home`*`\bin`
`system.db`	*`Data_Protector_program_data`*`\Config\client\StoreOnceSoftware`

Systèmes Linux :
suite à une installation réussie, StoreOnceSoftware est démarré en tant que processus d'arrière-plan (démon). Il peut être démarré automatiquement après un redémarrage.

Le composant d'installation comprend les fichiers suivants :

Nom de fichier	Emplacement du fichier
StoreOnceSoftware	/opt/omni/lbin
StoreOnceSoftwared	/etc/init.d/ /opt/omni/lbin
system.db	/etc/opt/omni/client/StoreOnceSoftware

Dépannage

Cette section traite des journaux et du rapport d'évènements, des avertissements, des diagnostics et des informations de dépannage dans le cadre de l'utilisation de l'intégration du logiciel Data Protector StoreOnce. Pour des informations générales concernant le dépannage Data Protector, consultez le *Guide de dépannage HP Data Protector*.

Avertissement d'espace disque faible

Pour éviter de manquer d'espace sur le disque hébergeant les banques, un message d'avertissement s'affiche (journal d'événements sur les systèmes Windows ou Syslog sur les systèmes Linux) lorsqu'un seuil prédéfini est atteint. La valeur par défaut du seuil est de 10% de la capacité de la banque. La valeur par défaut peut être modifiée à l'aide de l'option omnirc. Le message d'avertissement est émis avant toute opération de lecture/écriture supplémentaire, une fois par jour, ou lorsque l'utilitaire StoreOnceSoftware est redémarré. Un avertissement s'affiche également dans le message de session de sauvegarde au début et à la fin de la session. Le message d'avertissement d'espace disque faible est le suivant :

```
You are running out of disk space on Deduplication Store root directory: [path].
The threshold x% is reached. Please free space or add more disks. [warning].
```

Sauvegarde du fichier system.db

Le fichier de base de données `system.db` contient les informations de répertoire racine et des informations sur les banques. Il est situé dans *`DataProtector_Program_Data`*`\OmniBack\Config\client\StoreOnceSoftware`. Si ce fichier est effacé ou perdu, la banque et les données sauvegardées sont inaccessibles. Pour éviter cette situation, lors de chaque modification effectuée sur la base de données, une copie de sauvegarde du fichier `system.db` est faite dans `.\Store_Root\StoreOncelibrary\system.db.bak`. Le fichier `system.db` peut être restauré en copiant le fichier de sauvegarde dans l'emplacement d'origine, en le renommant, et en redémarrant l'utilitaire StoreOnceSoftware.

Vérifiez que les fichiers situés dans le répertoire racine sont protégés (RAID ou sauvegarde).

La liste suivante présente les erreurs et problèmes courants rapportés par l'utilitaire StoreOnceSoftware. Les erreurs sont généralement liées à l'environnement d'exploitation et à la structure de répertoire de la banque de déduplication.

L'utilitaire StoreOnceSoftware ne parvient pas à trouver le répertoire racine de la banque.

Problème
`Accessing the system.db file: The system.db file is inaccessible (for example, permission denied, or disk full).`
Action
Modifiez les permissions, l'espace disque libre, ou rendez la base de données accessible. Le fichier de base de données (`system.db`) contient une valeur vide ou ne contient aucune valeur pour le répertoire racine de la banque de déduplication.

L'utilitaire StoreOnceSoftware ne peut pas démarrer.

Problème
Accéder au fichier system.db : le fichier system.db du répertoire racine de la banque est introuvable.
Action
Restaurez ou recréez le fichier system.db. Voir le problème précédent.

Pendant le démarrage de la banque, une erreur est consignée dans le journal. Impossible d'accéder à la banque.

Problème
Démarrer les banques : le répertoire de banque est inaccessible.
Action
Rendez le répertoire de banque accessible, contrôlez les permissions, et vérifiez que le répertoire racine existe.

Le démarrage de la banque est réussi, mais aucun élément n'est détecté.

Problème
Démarrer les banques : le répertoire de banque est introuvable.
Action
Restaurez le répertoire racine et les banques situées en aval du répertoire racine.

Une erreur est consignée dans le journal. Impossible d'accéder à la banque.

Problème
Démarrer les banques : la banque est encrassée et ne peut être récupérée.
Action
Restaurez le répertoire racine et les banques situées en aval du répertoire racine.

L'arrêt de la banque renvoie une erreur.

Problème
Arrêter les banques : des éléments sont ouverts (par exemple, des sessions de sauvegarde ou de restauration sont en cours d'exécution).
Action
Vérifiez que toutes les opérations sont terminées avant d'arrêter l'utilitaire StoreOnceSoftware.

Une erreur est consignée dans le journal au cours de l'arrêt. La récupération peut survenir au prochain démarrage.

Problème
Arrêter les banques : l'utilitaire de gestion interne ne peut être arrêté.
Action
Vérifiez que toutes les opérations sont terminées, puis arrêtez l'utilitaire StoreOnceSoftware. La récupération peut survenir au prochain démarrage.

Lorsque l'espace disque est faible, un message d'avertissement sera consigné dans le journal.

Problème
Les messages d'avertissement et d'erreur sont consignés dans le journal d'évènements Windows ou le syslog Linux par le service/démon du logiciel StoreOnce en raison d'un faible espace disque et mémoire. Lorsque le système atteint le seuil de 25% de mémoire virtuelle restante, un message d'avertissement est consigné, et lorsque le seuil de 20% de mémoire virtuelle restante est atteint, un message d'erreur est consigné et le service/démon commence à rejeter les opérations de lecture et d'écriture.
Action
Libérez des ressources système. Le service/démon arrêtera de rejeter les opérations lorsque suffisamment d'espace disque ou de mémoire aura été libéré.

Data Protector affiche l'avertissement "La banque n'existe pas" et la session de sauvegarde échoue.

Problème
Lorsqu'il effectue une session de sauvegarde à l'aide d'un périphérique de système de sauvegarde StoreOnce, Data Protector affiche un avertissement similaire au suivant et la session s'arrête de manière anormale : `[Warning] From: BSM@computer.company.com "CS2BackupTmp" Time: 6/18/2012 1:34:08 PM Got error: " Store does not exist. " when contacting " DeviceName" B2D device!`

Ce problème peut survenir si la banque a été supprimée du périphérique B2D ou si les permissions pour cette banque ont été modifiées.
Action
• Vérifiez que la banque existe et si des permissions ont été modifiées pour cette banque. • Si la banque a été configurée correctement, vérifiez les paramètres du périphérique dans Data Protector. Cliquez sur le périphérique avec le bouton droit de la souris, sélectionnez Propriétés puis sur la page Périphériques - Banque et passerelles, vérifiez l'ID client.

Les mises à jour de l'état sur les périphériques B2D sont effectuées à intervalles réguliers.

Problème
Le quota logiciel de la taille de la sauvegarde ou le quota logiciel de la taille de la banque est dépassé mais Data Protector ne renvoie aucun avertissement.
Action
Aucune. La prochaine session de sauvegarde rapportera correctement les avertissements.

A propos des peripheriques de deduplication StoreOnce Store et DD Boost

Data Protector prend en charge les produits de déduplication de HPE (StoreOnce) et EMC (DD Boost). Catalyst est le logiciel qui gère la déduplication StoreOnce, et les deux termes sont utilisés de manière interchangeable dans ce qui suit. Pour plus d'informations, reportez-vous au *HPE Data ProtectorGuide conceptuel* .

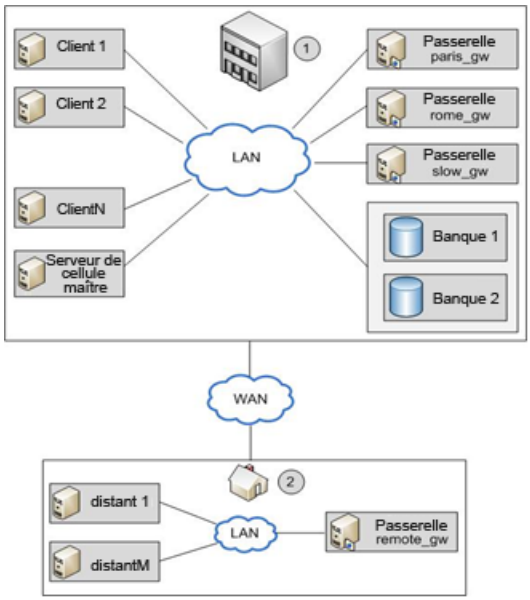
Cette section comprend un exemple d'environnement et de procédures de configuration.

Prise en charge multi-interface

Data Protector fournit une prise en charge multi-interface ; une connexion IP tout comme une connexion FC peut permettre d'accéder à la même banque Catalyst ou Boost. Data Protector prend en charge les connexions IP et Fiber Channel à la même banque Catalyst / DDBoost sans qu'il soit nécessaire de configurer une banque distincte. La banque est accessible simultanément via les deux interfaces. Par exemple, une même banque Catalyst / DDBoost peut être accessible aux clients locaux via une connexion Fiber Channel pour une sauvegarde plus rapide alors que les clients distants ont accès à la même banque via un réseau WAN pour une sauvegarde plus lente.

Exemple de configuration sur un périphérique B2D

La figure suivante présente un modèle type d'utilisation d'une configuration bureau central / bureau distant.



Elément	Description
1	Bureau central. Ce LAN est situé dans le bureau central. Il est connecté au LAN du bureau distant via un réseau WAN.
2	Bureau distant. Ce LAN est situé dans le bureau distant.

Le Gestionnaire de cellule Data Protector est installé dans le bureau central sur l'hôte *master*. Le bureau central héberge plusieurs clients : *client1 à clientN* (clients non passerelles), *paris_gw, rome_gw,* et *slow_gw* (clients passerelles). De plus, deux banques d'objets (Banque1 et Banque2) sont configurées dans le bureau central.

Le bureau distant comprend les clients *remote1* to *remoteM* et *remote_gw*. Tous les clients du bureau distant font partie de la même cellule Data Protector que les clients du bureau central. Le bureau distant est connecté au bureau central via un réseau WAN lent.

> **REMARQUE :**
> Les passerelles sont simplement des clients sur lesquels le composant Agent de support est installé. Considérez-les comme des clients de passerelles. Pour qu'un client devienne une passerelle, son système doit être en 64 bits.

Quand vous configurez un périphérique B2D, vous devez spécifier certains paramètres, comme le nom et l'emplacement de la banque, les passerelles, et les chemins d'accès réseau. Dans l'exemple ci-dessus, vous voulez utiliser la banque Banque1 (à laquelle on accède par déduplication du logiciel StoreOnce) pour la sauvegarde de clients de votre environnement. Pour ce faire, vous configurez le périphérique B2D pour utiliser Banque1 comme référentiel. Vous décidez également que les clients *paris_gw, rome_gw*, et *slow_gw* doivent être utilisés comme passerelles pour les autres clients Data Protector du bureau central. Veuillez également noter les points suivants :

- La simultanéité indique le nombre d'Agents de disque qui écrivent sur le périphérique en parallèle. Plusieurs Agents de disque lisent les données des disques en parallèle et les envoient à plusieurs Agents de support dans un flux constant de données. Avec la déduplication du logiciel StoreOnce,

la simultanéité des Agents de disque pour chaque Agent de support est définie sur 1 (cela améliore le taux de déduplication).

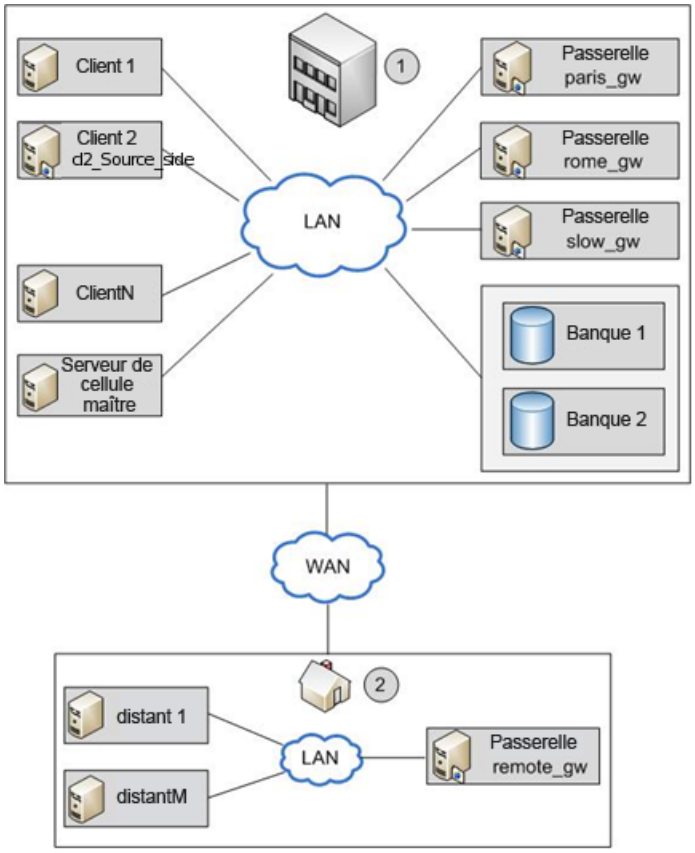
- Data Protector prend en charge la sauvegarde vers des banques non cryptées comme des banques cryptées. Le cryptage peut être activé au moment de la création de la banque. Notez qu'une fois la banque créée, il est impossible de changer son état de crypté à non crypté, ou inversement.
- Une seule banque peut être configurée pour chaque périphérique.
- Les banques sont représentées par des chemins d'accès réseau (UNC) qui contiennent des informations concernant le système de déduplication et le nom de la banque. (Remarque : dans le cadre des périphériques B2D, le système de déduplication fait référence au nom de la machine hôte hébergeant la banque de déduplication.)

Déduplication côté source

Le scénario ci-dessus fonctionne si la quantité de données sauvegardées depuis les clients distincts est limitée. Cependant, pour réduire le trafic sur le réseau, vous pouvez configurer des passerelles côté source.

Par exemple, dans notre scénario, client2 est un système où la quantité de données dupliquées est importante, mais où la charge du système est modérée. Pour réduire la charge réseau, vous pouvez activer la déduplication côté source pour le périphérique B2D. Si vous activez ensuite la déduplication côté source dans la spécification de sauvegarde du client2, une passerelle côté source sera automatiquement créée sur le client2 et l'Agent de support n'enverra que des données dédupliquées sur le réseau.

De la même façon, si vous activez la déduplication côté source pour d'autres clients, des passerelles côté source seront également créées sur ces clients.



Ajouter un périphérique B2D

La procédure pour ajouter un dispositif B2D est similaire à la procédure pour ajouter des types de dispositif. Pour plus d'informations, consultez l'*Aide en ligne HPE Data Protector*, et le *Guide de l'administrateur HPE Data Protector* .

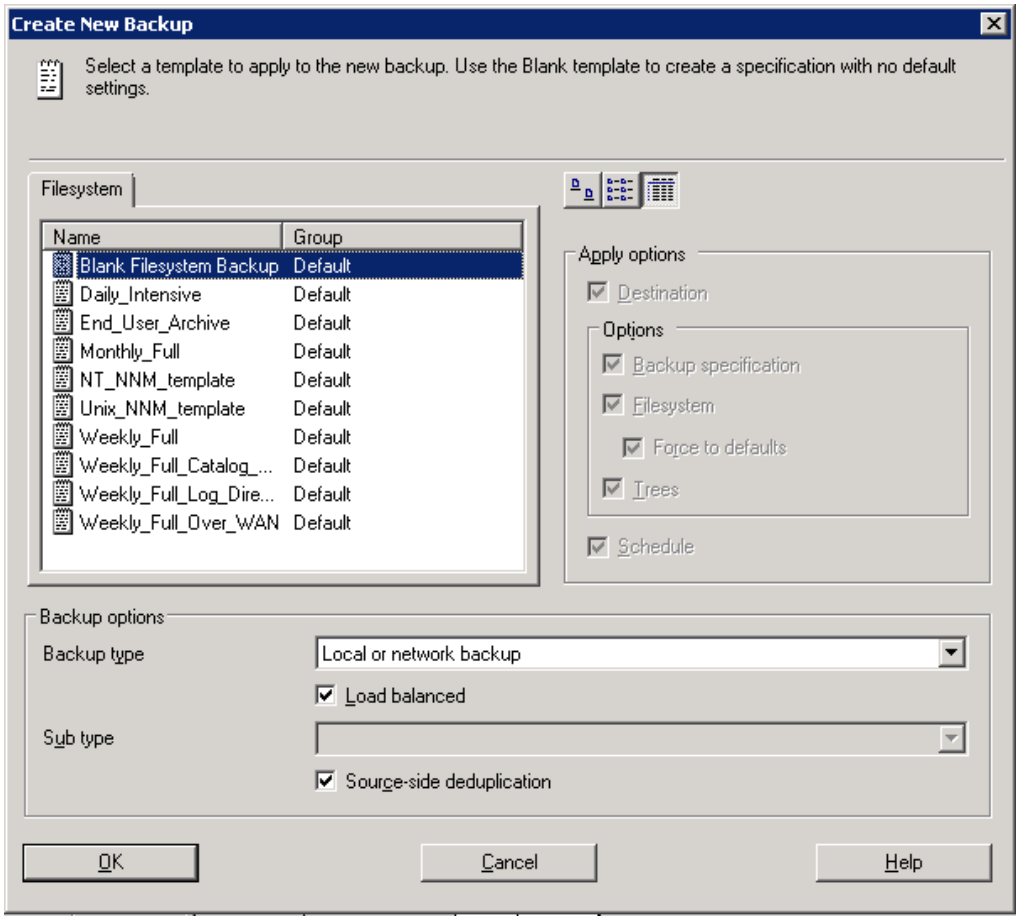
Sauvegarde

En spécifiant un périphérique B2D dans la spécification de sauvegarde, vous indiquez à Data Protector d'effectuer une sauvegarde de type déduplication Le processus de déduplication s'effectue en arrière-plan et les données dédupliquées sont écrites dans le système du logiciel StoreOnce ou le Système de sauvegarde StoreOnce.

Une sauvegarde de type déduplication s'effectue de la même manière qu'une sauvegarde classique :

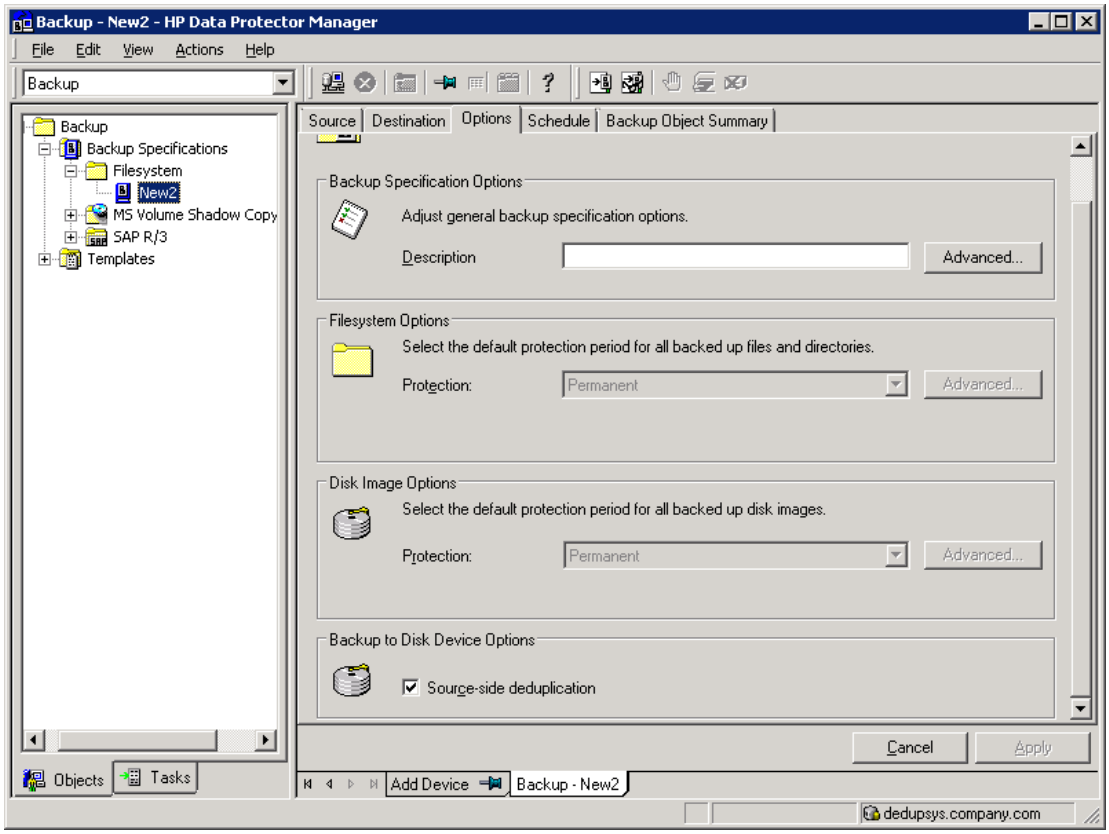
1. Ajoutez un Périphérique B2D (dans ce cas, en spécifiant Déduplication du logiciel StoreOnce ou Système de sauvegarde StoreOnce).
2. Créez une spécification de sauvegarde ciblant ce périphérique. Pour plus de détails, consultez l'index *Aide de HPE Data Protector* : « spécifications de création et de sauvegarde ». Vous pouvez, si vous le souhaitez, activer la déduplication côté source en sélectionnant l'option Déduplication côté source au moment de créer la spécification de

sauvegarde.



Lors de la sélection des objets de sauvegarde dans la page Source, Data Protector grisera tous les clients pour lesquels aucune passerelle côté source n'est configurée. Vous pouvez filtrer la liste des clients en sélectionnant **Déduplication côté source** dans la liste déroulante Montrer.

Autre alternative : sélectionnez la spécification de sauvegarde, ouvrez le panneau Options et sélectionnez **Déduplication côté source**.



3. Dans la page Destination, sélectionnez une passerelle à utiliser pour la sauvegarde. Cliquez sur **Propriétés** pour contrôler et modifier les options de passerelle. Notez qu'en spécifiant l'option **Nombre max. de flux parallèles par passerelle**, vous écrasez la valeur définie lors de la configuration du périphérique.

REMARQUE :
Lorsque la déduplication côté source est sélectionnée, vous ne pouvez sauvegarder des objets que depuis des clients prenant en charge les passerelles côté source, et vous ne pouvez sélectionner que les périphériques dotés de passerelles côté source. Si vous désélectionnez l'option, Data Protector sélectionnera automatiquement toutes les passerelles des périphériques B2D au lieu des passerelles côté source, et affichera un message d'avertissement.

IMPORTANT :
Si vous activez la déduplication côté source dans une spécification de sauvegarde existante, les clients où la déduplication côté source ne peut être effectuée seront désélectionnés et ne pourront être sauvegardés.

Restaurer

La restauration des données sauvegardées se fait de la même manière que pour une opération de restauration classique. Bien que le processus d'arrière-plan consistant à récupérer les données depuis la banque de déduplication soit assez différent des processus de restauration classiques, aucune tâche particulière n'est à effectuer. Les opérations principales du processus de récupération

comprennent le chargement sur la mémoire des données à restaurées, la lecture des informations de référence sur les tables d'index, et l'utilisation de ces informations pour *réhydrater* les données sauvegardées. Consultez l'index *Aide de HP Data Protector* : "restauration".

Considérations relatives à la déduplication côté source

Si la sauvegarde a été effectuée avec la déduplication côté source activée et que la restauration est effectuée vers un client sur lequel les passerelles côté source ne sont pas prises en charge, une passerelle ordinaire sera utilisée.

Configuration des clients StoreOnce Catalyst pour Catalyst sur Fibre Channel

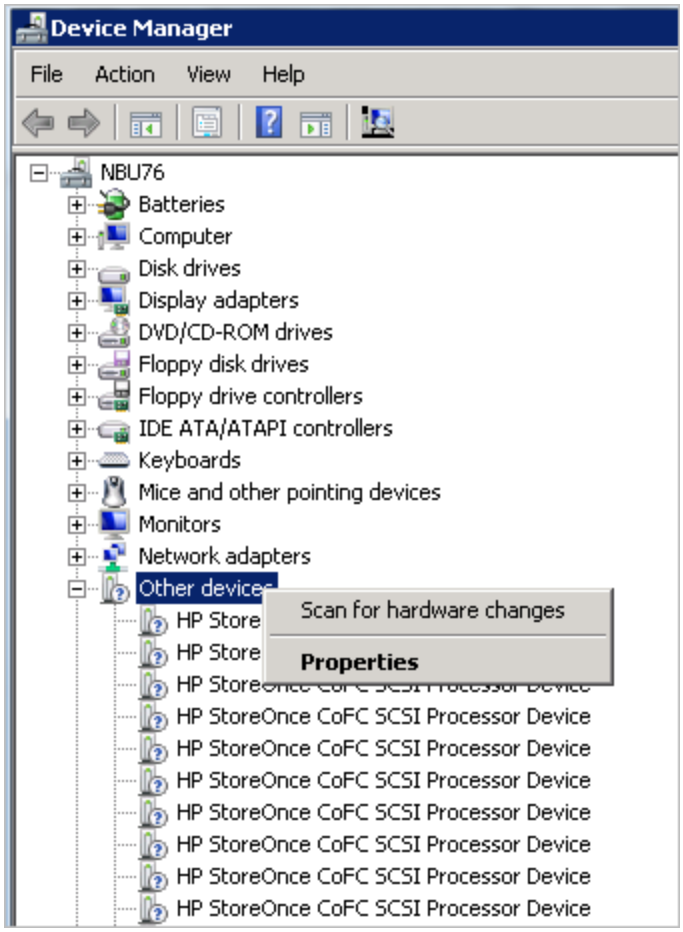
> **REMARQUE :**
> Les informations suivantes ne prétendent pas faire autorité. Pour les informations les plus récentes et les plus détaillées, consultez les documents StoreOnce.

Clients Windows

Les permissions Administrateur sont nécessaires pour lancer les sauvegardes Catalyst sur Fibre Channel.

StoreOnce Catalyst sur Fibre Channel présente un type de périphérique de **Processeur**. Après avoir zoné les périphériques ou changé le nombre de périphériques par port initiateur, procédez comme suit :

1. Allez au **Gestionnaire de périphériques Windows**, faites un clic droit sur **Autres périphériques**.
2. Sélectionnez **Rechercher les modifications sur le matériel** pour détecter les nouveaux périphériques.



Clients Linux

StoreOnce Catalyst sur Fibre Channel présente un type de périphérique de Processeur. Sous Linux, les fichiers de périphérique sont créés dans `/dev/sg*`. Par défaut, les périphériques `/dev/sg*` ne sont accessibles que par les utilisateurs root. Pour un utilisateur non root, fournissez à l'opérateur de sauvegarde des permissions pour accéder aux fichiers de périphérique à l'aide d'une règle udev Linux.

Pour créer une règle udev, procédez comme suit :

a. Créez un fichier udev dans l'emplacement suivant sur chacun des serveurs de sauvegarde :

   `/etc/udev/rules.d/70-cofc.rules`

b. Ajoutez la règle suivante au fichier :

   ```
   KERNEL=="sg[0-9]*", ATTRS{vendor}=="HP*", ATTRS{model}=="StoreOnce CoFC*",
   ATTRS{rev}=="CAT1", GROUP="##CORRECT_USER_GROUP##"
   ```

   Où `##CORRECT_USER_GROUP##` est remplacé par le groupe d'utilisateurs Linux qui effectuera les sauvegardes et les restaurations. Par exemple, `dba/oracle`.

c. Recherchez les modifications sur les fichiers de périphérique pour mettre à jour les permissions.

La commande `lsscsi --generic` peut être utilisée pour déterminer quels fichiers de périphériques /dev/sg* appartiennent à Catalyst sur Fibre Channel.

Clients AIX

Dans les versions du logiciel StoreOnce antérieures à la version 3.14, StoreOnce Catalyst sur Fibre Channel sur AIX n'est disponible que sur requête.

> **REMARQUE :**
> Si vous avez besoin de Catalyst sur Fibre Channel sur AIX 6.1 ou 7.1 avec des versions StoreOnce antérieures à la 3.14, contactez l'assistance StoreOnce.

StoreOnce Catalyst sur Fibre Channel présente un type de périphérique Séquentiel sur AIX. Ces fichiers de périphérique sont créés dans l'emplacement `/dev/rmt*`. Après avoir zoné les périphériques ou changé le nombre de périphériques par port initiateur, procédez comme suit :

a. Exécutez le script `storeonce-cofc-passthrough-install.sh`.

> **REMARQUE :**
> Ce script d'installation fait partie du kit du logiciel StoreOnce, et non d'HPE Data Protector.

b. Exécutez la commande `cfgmgr` en tant qu'utilisateur root pour recherchez les modifications dans le fichier de périphérique.

c. Par défaut, les fichiers de périphérique `/dev/rmt*` ne sont accessibles que par les utilisateurs root. Pour lancer des sauvegardes en tant qu'utilisateur non root, des permissions supplémentaires sont nécessaires.

Clients HP-UX

StoreOnce Catalyst sur Fibre Channel présente un type de périphérique de Processeur. Sur HP-UX, les fichiers de périphérique sont créés dans l'emplacement `/dev/pt/ptX`.

Après avoir zoné les périphériques ou changé le nombre de périphériques par port initiateur, procédez comme suit :

a. Recherchez les modifications sur les fichiers de périphérique.

b. Exécutez la commande `ioscan -fnC /dev/pt` en tant qu'utilisateur root.

Par défaut, les périphériques `/dev/pt/ptX` ne sont accessibles que par les utilisateurs root. Pour un utilisateur non root, fournissez à l'opérateur de sauvegarde des permissions pour accéder aux fichiers de périphérique à l'aide de la commande `chmod o+rwx /dev/pt/pt*` .

c. Pour obtenir les permissions pour les fichiers de périphérique /dev/pt/ptX, utilisez les commandes Catalyst sur Fibre Channel :

```
/usr/sbin/scsimgr -p get_attr all_lun -a device_file -a dev_type -a pid | grep StoreOnce
```

d. Utilisez la commande chmod o+rwx sur les périphériques appropriés.

Clients Solaris

StoreOnce Catalyst sur Fibre Channel présente un type de périphérique de Processeur. Sur Solaris, les fichiers de périphérique sont créés dans l'emplacement /dev/scsi/processor/*. Après avoir zoné les périphériques ou changé le nombre de périphériques par port initiateur, procédez comme suit :

a. Recherchez les modifications sur les fichiers de périphérique.
b. Si vous êtes un utilisateur root, exécutez les commandes suivantes :
   - `add_drv -vi scsiclass,03 sgen`
   - `update_drv -vai scsiclass,03 sgen`

     Par défaut, les périphériques /dev/scsi/processor/* ne sont accessibles que par les utilisateurs root. Pour un utilisateur non root, fournissez à l'opérateur de sauvegarde des permissions pour accéder aux fichiers de périphérique à l'aide de la commande `chmod -R o+rwx /dev/scsi/processor/*`.
c. Pour obtenir les permissions pour les fichiers de périphérique /dev/scsi/processor/*, utilisez les commandes Catalyst sur Fibre Channel :

   ```
   for i in /dev/scsi/processor/*; do echo $i; ls $i; luxadm inq $i | egrep "Vendor|Product"; echo; done
   ```
d. Utilisez la commande chmod -R o+rwx sur les périphériques appropriés.

Options omnirc liées aux périphériques B2D

Le fichier omnirc est amélioré par des options supplémentaires. Utilisez ce fichier pour définir des paramètres tels que le numéro de port et les avertissements de seuil d'espace disque.

`OB2_STOREONCESOFTWARE_COMMAND_PORT=`*`PortNumber`*

Cette option modifie le port utilisé pour la communication de commande entre l'Agent de support et l'utilitaire StoreOnceSoftware.

Par exemple : `OB2_STOREONCESOFTWARE_COMMAND_PORT=12345`

Valeur par défaut : 9387

`OB2_STOREONCESOFTWARE_DATA_PORT=`*`PortNumber`*

Cette option modifie le port utilisé pour la communication de données entre l'Agent de support et l'utilitaire StoreOnceSoftware.

Par exemple : `OB2_STOREONCESOFTWARE_DATA_PORT=12346`

Valeur par défaut : 9388

`OB2_STOREONCESOFTWARE_SESSION_IDLE_TIMEOUT=s`

Le démon StoreOnceSoftware recherche à intervalles réguliers les éventuelles connexions inactives, et y met fin. Cette option spécifie le nombre de secondes d'inactivité après lequel une connexion est considérée comme inactive.

Valeur par défaut : 300 (Plage : Minimum : 10)

`OB2_STOREONCESOFTWARE_DISK_SPACE_THRESHOLD=%`

Cette option sert à définir un seuil d'espace disque non utilisé.

Valeur par défaut : 10% (Plage : 1% - 95%)

`OB2_STOREONCESOFTWARE_MINIMUM_DISK_SPACE=n`

Cette option contrôle l'espace disque minimum (en Mo) que StoreOnceSoftware doit réserver. Si ce minimum est atteint, l'écriture de données échouera sur toutes les banques. Valeur par défaut : 1000 (Minimum : 500)

`OB2_STOREONCESOFTWARE_SSL_ENABLE=0|1`

Valeur par défaut : 1

Cette option active ou désactive la communication contrôlée par cryptage entre le client et le démon du logiciel StoreOnce. Notez que même si le client sur lequel le démon du logiciel StoreOnce s'exécute utilise la communication contrôlée par cryptage, celle-ci ne sera pas utilisée si vous définissez cette option sur 0.

Après avoir activé la communication sécurisée, redémarrer le démon StoreOnceSoftware manuellement.

`OB2_STOREONCESOFTWARE_DISABLE_IPV6_LISTEN=0|1`

Valeur par défaut : 0

Par défaut, le démon du logiciel StoreOnce apparaît sur un socket double (IPv6 et IPv4 sur le même port). Si cette option est définie sur 1, l'IPv6 est désactivée. Cette option s'applique aux ports d'écoute RPC et IpcServer.

`OB2D2D_COMMAND_PORT=PortNumber`

Cette option modifie le port utilisé pour la communication de commande entre l'Agent de support et le système de sauvegarde StoreOnce.

Par exemple : `OB2D2D_COMMAND_PORT =12345`

Valeur par défaut : 9387

`OB2D2D_DATA_PORT=PortNumber`

Cette option modifie le port utilisé pour la communication de données entre l'Agent de support et le système de sauvegarde StoreOnce.

Par exemple : `OB2D2D_DATA_PORT=12346`

Valeur par défaut : 9388

`OB2D2D_NUM_OF_LBWTHREADS=ThreadNum`

Définit le nombre de threads utilisés pour le calcul de la déduplication lorsque la déduplication est effectuée sur le client d'Agent de support. Si vous disposez d'une passerelle plus puissante, vous pouvez augmenter ce nombre jusqu'à 8 threads. Cette option doit être définie individuellement sur chaque passerelle.

Valeur par défaut : 4

`OB2D2D_BANDWIDTH_BUFF_SIZE=Size`

Définit la taille de mémoire tampon lorsque la déduplication est effectuée sur un client d'Agent de support. La valeur par défaut est appropriée quand l'Agent de support communique avec le périphérique D2D via le LAN. Lorsqu'un réseau WAN est utilisé pour la communication, 20 Mo est une valeur plus appropriée. Cette option doit être définie individuellement sur chaque passerelle.

Valeur par défaut : 10 Mo.

À propos des périphériques de cloud (Helion)

Un périphérique de cloud (Helion) est un périphérique configuré avec les informations d'identification cloud (Helion) et qui prend en charge le cloud public de HPE. L'agent de support a été amélioré pour prendre le rôle de passerelle de cloud pour transmettre des données au périphérique de cloud (Helion). Il se comporte de la même manière qu'un périphérique de sauvegarde sur disque (B2D).

Conditions préalables

Conditions préalables dans le cloud public HPE :

- Vous devez disposer d'un compte et d'identifiants de Cloud public HPE. Pour plus d'informations, consultez le site https://horizon.hpcloud.com.
- Vous devez avoir souscrit à la Banque d'objets du Cloud public HPE.
- Pour votre projet dans le Cloud public HPE, vous devez noter le nom du projet.
- URL du service d'authentification de la région géographique la plus proche de votre centre de données.
- Si vous décidez d'utiliser les clés d'accès pour l'authentification au lieu des informations d'identification (identifiant et mot de passe), créez vos clés d'accès dans le Cloud Public HPE.

Conditions préalables dans Data Protector :

- Vérifiez que les dernières versions du Gestionnaire de cellule, du client d'interface utilisateur et du serveur d'installation de Data Protector sont installées sur les systèmes pris en charge, avec le dernier paquet General Patch Release 9.04.

Pour plus de détails, consultez les dernières matrices de prise en charge HPE Data Protector sur https://softwaresupport.hpe.com/. Voir le *Guide d'installation HPE Data Protector* pour installer HPE Data Protector dans différentes architectures.

- Installez l'Agent de support ou l'Agent de support NDMP de Data Protector sur les systèmes Windows et Linux voués à devenir des passerelles de cloud, y compris sur les clients sur lesquels le périphérique de cloud Helion sera activé. Pour plus d'instructions, voir le *Guide d'installation HPE Data Protector*.

  Pour consulter une liste détaillée des versions de systèmes d'exploitation prises en charge, consultez les dernières matrices de prise en charge sur https://softwaresupport.hpe.com/.

Limites

- La copie d'objets de périphériques de cloud (Helion) a été testée, et est prise en charge par les périphériques suivants :
  - Périphériques source : périphériques de bibliothèque de fichiers et périphériques StoreOnce.
  - Spécifications de sauvegarde VMware.
- Lorsque vous choisissez ou créez un conteneur dans la banque d'objets HPE, les restrictions suivantes s'appliquent :
  - Chaque périphérique ne peut avoir qu'un seul conteneur affecté.
  - Plusieurs périphériques ne peuvent utiliser le même conteneur.
  - Une fois affecté à un périphérique, un conteneur ne peut pas être modifié.
- Lorsque vous configurez le périphérique de cloud (Helion), vérifiez que sa taille de bloc est supérieure ou égale à celle du périphérique source sur site.

  Si vous envisagez d'effectuer des copies d'objets d'un périphérique à l'autre - périphérique sur site et périphérique de cloud (Helion) - la taille de bloc des deux périphériques doit être identique. La taille de bloc peut être définie dans les propriétés de la passerelle.

Recommandations

HPE recommande les mesures suivantes pour les périphériques de cloud (Helion) :

- Lors de la sauvegarde de spécification VMware, utilisez une passerelle de cloud locale vers la source de données car cela réduira la charge réseau pendant les opérations de copie des objets.
- Utilisez si possible des **clés d'accès** comme mode d'authentification. Ce mode limite l'accès au périphérique de cloud (Helion) et il est plus sûr, du fait qu'il est généré par le système.
- Divisez les grands jeux de données en spécifications de sauvegarde multiples lors de la copie de données vers le cloud HPE.

  Cela permet de lancer de nombreuses sessions de copie en parallèle, d'augmenter l'utilisation globale de bande passante et d'effectuer des copies de données plus efficaces sur le cloud HPE.
- La consolidation sur le périphérique de cloud (Helion) n'est pas recommandée, en raison des grandes exigences sur la bande passante et des coûts associés sur le cloud HPE.

Préparer le périphérique de cloud (Helion)

Les tâches suivantes doivent être réalisées pour configurer les opérations de copie d'objets vers le périphérique de cloud (Helion).

1. Configurez une spécification de sauvegarde pour sauvegarder vos données sur un périphérique de sauvegarde local. Pour plus d'informations, voir Création d'une spécification de sauvegarde.
2. Dans le cloud public HPE, récupérez vos identifiants de compte utilisateur ou les clés d'accès nécessaires à l'authentification, ainsi que l'URL du service d'authentification et des autres éléments nécessaires pour le cloud public HPE, et souscrivez à la banque d'objets. Ces éléments serviront à configurer le périphérique de cloud (Helion).
3. Dans HPE Data Protector, configurez un périphérique de cloud (Helion). Pour plus d'informations, voir Configuration de périphériques de cloud.
4. Configurez les sessions de copie d'objets à l'aide du périphérique de sauvegarde local en tant que périphérique source, et le périphérique de cloud (Helion) en tant que périphérique de sauvegarde de destination.

   La création d'une copie d'une opération d'objet de périphérique de cloud (Helion) permet aux données stockées sur le périphérique de sauvegarde local de répliquer des données vers le cloud public HPE. Les données envoyées vers le périphérique de cloud (Helion) sont compressées et cryptées par défaut.
5. Pour restaurer des données depuis le périphérique de cloud (Helion), vous pouvez utiliser une des méthodes suivantes :
   - Créez une copie d'objet depuis le périphérique de cloud (Helion) vers votre périphérique de sauvegarde local, et restaurez vers votre client depuis le périphérique de sauvegarde local.
   - Recyclez et exportez le support local et restaurez directement depuis le périphérique de cloud (Helion) vers votre client.
   - Restaurez directement depuis le cloud (Helion), même si des versions locales existent, en spécifiant le périphérique de cloud (Helion) à utiliser pour la restauration.
   - Définissez la priorité d'emplacement du support sur le support de cloud (Helion), plutôt que sur le support local. Voir Définition de la priorité des emplacements des supports.

À propos des périphériques de cloud (Azure)

Un nouveau périphérique de cloud est utilisé pour activer la copie d'objet vers le stockage d'objet Microsoft Azure à partir de Data Protector. Le périphérique de cloud (Azure) est configuré avec les identifiants Azure et il envoie des données sur le cloud.

Conditions préalables

Conditions préalables dans le portail de périphériques du cloud (Azure)

- Vous devez disposer d'un compte Microsoft Azure. Pour plus d'informations, consultez le portail Microsoft Azure.
- Vous devez disposer de deux clés d'accès de stockage, que Microsoft Azure génère au moment de la création du compte de stockage Microsoft Azure.

  Deux clés d'accès sont générées pour le compte. Ces clés sont nécessaires lors de la création du périphérique Data Protector associé, dans le cadre du processus de fourniture des informations d'identification.
- L'horodatage du système doit être correctement réglé afin de s'assurer d'une bonne synchronisation entre l'hôte passerelle et Microsoft Azure.

Conditions préalables dansData Protector :

- Vérifiez que le Gestionnaire de cellule, le client d'interface utilisateur et le serveur d'installation de Data Protector sont installés sur des systèmes pris en charge, avec le dernier paquet General Patch Release.

  Pour plus d'informations sur l'installation de HPE Data Protector sur diverses architectures, consultez le *Guide d'installation HPE Data Protector*.
- Installez l'Agent de support ou l'Agent de support NDMP de Data Protector sur les systèmes Windows et Linux voués à devenir des passerelles de cloud (Azure), y compris sur les clients sur lesquels le périphérique de cloud (Azure) sera activé. Pour des instructions détaillées, consultez le *Guide d'installation HP Data Protector*.

  Pour obtenir une liste détaillée des versions de systèmes d'exploitation pris en charge, consultez les dernières matrices de prise en charge sur https://softwaresupport.hpe.com/manuals.

  > **REMARQUE :**
  >
  > - Dans le cas où des systèmes d'agent de support nécessiteraient la configuration d'un serveur proxy pour la connexion web, `omnirc` la variable `OB2_CLOUD_DEVICE_PROXY=<proxy_server:port_number>` doit être configurée dans le fichier `omnirc` .
  > - Les Agents de support disposent d'un mécanisme interne de nouvelle tentative, afin de faire face à diverses conditions d'erreurs. Par conséquent, les opérations utilisateur peuvent parfois prendre un certain temps. De tels problèmes ne devraient pas survenir en temps normal.

Limites

Les limites concernant les périphériques de cloud (Azure) sont les suivantes :

- La copie d'objets des périphériques de cloud (Azure) est prise en charge par les périphériques suivants :
  - Périphériques source : périphériques de bibliothèque de fichiers et périphériques StoreOnce.
  - Spécifications de sauvegarde du système de fichiers
- Lorsque vous choisissez ou créez un conteneur sur un périphérique de cloud (Azure), les restrictions suivantes s'appliquent :

- Chaque périphérique ne peut avoir qu'un seul conteneur affecté.
- Un même conteneur ne peut être utilisé par des périphériques multiples.
- Une fois affecté à un périphérique, un conteneur ne peut pas être modifié.

Taille limite de blob de périphérique de cloud (Azure)

Un support Data Protector est téléchargé sur le périphérique de cloud (Azure) sous forme d'un ou plusieurs blob(s) de données et de métadonnées. Le cloud (Azure) a une limite de taille de blob de 195 GB, tandis que les supports Data Protector n'ont pas de limite maximale. Cependant, pour s'adapter à ces restrictions, un support Data Protector peut s'étendre sur des plusieurs blobs, dont la taille ne dépasse pas 75 GB. La quantité exacte de données stockée par blob est fonction de la compression des données.

Recommandations

Les recommandations de configuration des périphériques de cloud (Azure) sont les suivantes :

- Lors de la sauvegarde des spécifications du système de fichiers, utilisez une passerelle de périphérique de cloud (Azure) locale à la source de données, afin de réduire la charge réseau au cours des opérations de copie d'objets.
- Étant donné que les tâches de copie d'objets vers le cloud (Azure) sont cryptées par défaut, le cryptage doit être désactivé dans les spécifications de sauvegarde initiales qui génèrent les données pour l'opération de copie. Si le cryptage est activé (ON), les données sont cryptées deux fois, des ressources CPU sont consommées, et les données de copie d'objets deviennent incompressibles. Par conséquent, la quantité de données transférées au cloud (Azure) augmente, ce qui allonge les temps de copie.
- Divisez les grands jeux de données en spécifications de sauvegardes multiples lors de la copie de données vers un périphérique de cloud (Azure), afin de pouvoir activer plusieurs sessions de copie en parallèle. Ainsi, la bande passante générale est améliorée.
- La consolidation sur périphérique de cloud (Azure) n'est pas recommandée, en raison des grandes exigences sur la bande passante et des coûts associés.

Préparer le périphérique de cloud (Azure)

Les tâches suivantes doivent être réalisées pour configurer les opérations de copie d'objets vers un périphérique de cloud (Azure).

1. Configurez une spécification de sauvegarde pour sauvegarder vos données sur un périphérique de sauvegarde local. Pour plus d'informations, reportez-vous à Création d'une spécification de sauvegarde, Page 303
2. Connectez-vous au portail Microsoft Azure et récupérez les clés d'accès nécessaires à l'utilisation du compte de stockage Microsoft Azure.
3. Configurez le périphérique de cloud (Azure) dans Data Protector. Pour plus d'informations, reportez-vous à Configuration d'un périphérique de sauvegarde sur disque - Cloud (Azure), Page 190.
4. Configurez les sessions de copie d'objets à l'aide du périphérique de sauvegarde local en tant que

périphérique source, et le périphérique de cloud (Azure) en tant que périphérique de sauvegarde de destination.

La création d'une copie d'une opération d'objet de périphérique de cloud (Azure) permet aux données stockées sur le périphérique de sauvegarde local de répliquer des données vers le périphérique de cloud (Azure). Les données envoyées au cloud (Azure) sont compressées et cryptées par défaut.

5. Restaurer des données depuis un périphérique de cloud (Azure). Pour restaurer, vous pouvez utiliser une des méthodes suivantes :
   - Créez une copie d'objet depuis le périphérique de cloud (Azure) vers votre périphérique de sauvegarde local, et restaurez vers votre client depuis le périphérique de sauvegarde local.
   - Recyclez et exportez le support local et restaurez directement depuis le périphérique de cloud (Azure) vers votre client.
   - Restaurez directement depuis le cloud (Azure), même si des versions locales existent, en spécifiant le périphérique de cloud (Azure) à utiliser pour la restauration.
   - Définissez la priorité d'emplacement du support sur le support de cloud (Azure), plutôt que sur le support local. Voir Définition de la priorité d'emplacement des supports, Page 284.

Réglage des performances du périphérique

Taille de bloc

Vous pouvez configurer chaque périphérique logique de manière à traiter les données sous la forme d'unités de taille spécifique (taille de bloc). Les tailles de bloc par défaut diffèrent en fonction des périphériques ; elles sont utilisables (toutes les sessions sont exécutées correctement) mais elles peuvent ne pas être optimales. En modifiant la taille de bloc, vous pouvez améliorer les performances des sessions Data Protector.

La valeur optimale de la taille de bloc dépend de votre environnement :

- Matériel (périphériques, passerelles, commutateurs, etc.)
- Microprogrammes
- Logiciels (système d'exploitation, pilotes, pare-feu, etc.)

Pour obtenir des résultats optimaux, vous devez optimiser votre environnement en installant la dernière version des pilotes et des microprogrammes, puis optimiser votre réseau et ainsi de suite.

Déterminer la taille de bloc optimale

Pour déterminer la taille de bloc optimale, faites des tests et exécutez des tâches Data Protector courantes (sauvegarde, restauration, copie, etc.) en utilisant des tailles différentes, puis mesurez les performances.

> **REMARQUE :**
> Une fois que vous avez modifié la taille de bloc sur un périphérique, vous ne pouvez plus

> restaurer les anciennes sauvegardes (effectuées avec l'ancienne taille de bloc) au moyen de ce périphérique. .
>
> Vous devez donc conserver vos anciens périphériques logiques et pools de supports en l'état afin de pouvoir restaurer les données de l'ancien support, et créer de nouveaux périphériques logiques et pools de supports pour vos tests. Au sinon, apprenez comment changer la taille du bloc lors de la restauration. La boîte de dialogue de restauration vous invite à spécifier une la taille de bloc.

Limites

- Récupération de sinistre : Afin de pouvoir réaliser une récupération EADR/OBDR hors ligne (Récupération de Sinistre Automatisée Améliorée, Récupération de Sinistre à Une Touche), sauvegardez vos données à l'aide de la taille de bloc par défaut.
- Bibliothèque : si vous utilisez plusieurs types de disque de technologie similaire dans la même bibliothèque, les disques doivent avoir la même taille de bloc.
- Adaptateurs SCSI : Vérifiez si la taille de bloc sélectionnée est prise en charge par l'adapateur SCSI de l'host auquel le dispositif est connecté.
- Fonctionnalité copie de l'objet : Les dispositifs de destination doivent avoir une taille de bloc identique ou supérieure que les dispositifs sources.
- Fonctionnalité consolidation de l'objet : Les dispositifs de destination doivent avoir une taille de bloc identique ou supérieure que les dispositifs sources.
- Miroir : La taille de bloc des dispositifs ne doit pas diminuer avec la chaîne de mirroir. La taille de bloc des périphériques utilisés pour la mise en miroir 1 doit être égale ou supérieure à celle des périphériques utilisés pour la sauvegarde. La taille de bloc des périphériques utilisés pour la mise en miroir 2 doit être supérieure ou égale à celle des périphériques utilisés pour la mise en miroir 1, et ainsi de suite.

Pour d'autres restrictions, consultez le *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*.

Modification de la taille de bloc

Vous pouvez définir la taille de bloc dans l'onglet Tailles de la boîte de dialogue Options Avancées pour un dispositif spécifique. Pour plus d'informations, voir Définition des options avancées des périphériques et des supports.

Performances du périphérique

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

Les taux de transfert de données dépendent également de l'utilisation de la compression matérielle. Le taux de compression réalisable dépend de la nature des données sauvegardées. Dans la plupart des

cas, l'utilisation de périphériques rapides et de la compression matérielle permet d'améliorer les performances. Toutefois, cela n'est vrai que si les périphériques fonctionnent en mode continu.

Au début et à la fin d'une session de sauvegarde, les périphériques de sauvegarde exigent un temps supplémentaire pour des opérations comme le rembobinage du support et son montage ou son démontage.

Les bibliothèques présentent l'avantage d'être automatisées : lors de la sauvegarde, des supports nouveaux ou ayant déjà été utilisés doivent être chargés et lors de la restauration, ces supports doivent être accessibles rapidement. L'accès à la bibliothèque étant automatisé, ce processus est plus rapide.

Les périphériques de type disque sont plus rapides à utiliser que les autres. Lorsque vous utilisez un périphérique sur disque, plus besoin de monter ou de démonter les supports et l'accès aux données est plus rapide ce qui réduit les temps de sauvegarde et de restauration.

Prise en charge de nouveaux périphériques

Utiliser un dispositif qui ne figure pas dans la liste comme étant pris en charge dans le *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*, utilisez le fichier `scsitab`.

Le fichier `scsitab` est un formulaire lisible sur machine de la Matrice d'AssistanceHPE Data Protector et comprend des informations sur tous les dispositifs pris en charge. Le fichier `scsitab` est utilisé par l'Agent de Support HPE Data Protector pour déterminer si un dispositif ou une bibliothèque donné(e) est pris(e) en charge ou non. Il fournit également des informations sur le périphérique ainsi et ses paramètres spécifiques.

> **IMPORTANT :**
> La modification du fichier `scsitab` n'est pas prise en charge.

Pour utiliser un dispositif qui ne figure pas dans la liste comme étant pris en charge dans le *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*, téléchargez le dernier package de logiciel pour le fichier `scsitab` à partir du site internet HPE Data Protector à http://www.hpe.com/software/dataprotector.

Une fois que vous avez téléchargé le package de logiciel `scsitab`, suivez la procédure d'installation fournie avec le package de logiciel.

Le fichier `scsitab` se trouve sur le système auquel le dispositif est connecté, à l'emplacement suivant :

Systèmes Windows : *répertoire_Data_Protector*`\scsitab`

Systèmes HP-UX, Solaris et Linux : `/opt/omni/scsitab`

Autres systèmes UNIX : `/usr/omni/scsitab`

Si vous continuez à recevoir la même erreur lors de la configuration du périphérique, contactez le support HPE pour savoir quand le périphérique sera pris en charge.

Préparation des périphériques de sauvegarde

La préparation d'un périphérique de sauvegarde consiste à connecter le périphérique au système ou, dans un environnement SAN, au système SAN, et à identifier lequel des fichiers de périphériques associés (actifs) doit être utilisé (adresse SCSI).

Conditions préalables

Un Agent de support (l'Agent de support général ou l'Agent de support NDMP) doit être installé sur chaque système auquel est connecté un périphérique de sauvegarde ou, dans un environnement SAN, aux systèmes contrôlant les périphériques de sauvegarde sur le SAN.

Procédure

1. Connectez le périphérique de sauvegarde à un système informatique ou, dans un environnement SA, au système SAN.
2. Continuez la préparation :

   Systèmes Windows :

   Spécifiez la syntaxe de l'adresse SCSI d'un périphérique connecté au système Windows.

   Systèmes UNIX :

   Recherchez ou créez le nom de fichier de périphérique d'un périphérique connecté au système UNIX.
3. Si plusieurs périphériques utiliseront le même support, vous devez vous assurer que les paramètres de densité d'écriture et de taille de blocs sont identiques.
4. Démarrez le système afin que le périphérique soit connu par le système.
5. Pour certains périphériques de sauvegarde, des étapes supplémentaires doivent être effectuées.

Une fois le périphérique de sauvegarde préparé, configurez-le pour une utilisation avec Data Protector. Préparez les supports que vous souhaitez utiliser pour vos sauvegardes.

- Dans l'environnement SAN
- Périphériques de fichier
- Magasin
- Bibliothèque SCSI, bibliothèque de bandes magnéto-optiques, contrôle externe
- Pilotes de robots Windows

Dans l'environnement SAN

Procédure

1. Vérifiez que le même nom de fichier de périphérique de robot existe sur tous les systèmes qui ont besoin d'accéder à la bibliothèque partagée. Ignorez cette étape si vous prévoyez d'utiliser l'accès indirect à la bibliothèque.

   Systèmes HP-UX et Solaris :

   L'identité du fichier de périphérique est vérifiée via des liens matériels ou logiciels, si nécessaire.

   Systèmes Windows :

   Utilisez le fichier texte `libtab`pour remplacer l'identification du périphérique SCSI par défaut et réaffecter les périphériques de contrôle des robots aux lecteurs logiques définis sur un autre hôte.

Le fichier `libtab`devrait être créé sur le client Agent de support dans le répertoire *répertoire_Data_Protector*, sous forme de fichier texte avec la syntaxe suivante (les espaces dans le nom du lecteur logique sont autorisés) :

hostnamecontrol_device_filedevice_name

par exemple

```
computer.company.com scsi2:0:4:0 DLT_1
```

Périphériques de fichier

Désactivez l'option de compression de Windows pour un fichier que vous souhaitez utiliser comme périphérique. Vous pouvez le faire en utilisant l'Explorateur Windows :

Procédure

1. Cliquez avec le bouton droit sur le fichier, choisissez **Propriétés,** puis désactivez l'option **Compresser** sous **Attributs**.

Magasin

Procédure

1. Créez un pool de supports avec prise en charge des magasins avant de configurer un périphérique de magasin. Le périphérique doit prendre en charge les magasins (par exemple, HPE 12000e).

Bibliothèque SCSI, bibliothèque de bandes magnéto-optiques, contrôle externe

Procédure

1. Choisissez les emplacements de la bibliothèque que vous souhaitez utiliser avec Data Protector. Vous devrez les spécifier lors de la configuration d'une bibliothèque.

Pilotes de robots Windows

Sur les systèmes Windows, les pilotes de robots sont automatiquement chargés pour les bibliothèques à bandes activées. Pour utiliser les robots de bibliothèque avec Data Protector sur un système Windows, désactivez le pilote Windows correspondant.

Procédure

1. Dans le Panneau de configuration Windows, double-cliquez sur **Outils d'administration**.
2. Double-cliquez sur **Gestion de l'ordinateur**, puis cliquez sur **Gestionnaire de périphériques**.
3. Développez **Changeurs de support**.
4. Cliquez sur le changeur de support avec le bouton droit de la souris, puis sélectionnez **Désactiver**.

5. Redémarrez le système pour appliquer les changements. Les robots sont maintenant prêts à être configurés avec Data Protector.

Création d'adresses SCSI sur les systèmes Windows

La syntaxe d'une adresse SCSI dépend du type de périphérique physique (magnéto-optique ou à bandes) connecté à votre système Windows. Le périphérique doit être connecté au système (et mis sous tension) avant l'amorçage de ce dernier.

> **CONSEIL :**
> Vous pouvez détecter automatiquement les adresses SCSI avec Data Protector.

Périphérique magnéto-optique

Si un dispositif magnéto-optique est connecté à votre système, la syntaxe d'adresse SCSI est `N:B:T:P:L` (`N`=mountpoint du disque amovible, `B`=numéro Bus, `T`=ID Cible SCSI, `P`=chemin d'accès, `L`=LUN).

Ouvrez **Cartes SCSI** dans le **Panneau de configuration** et cliquez deux fois sur le nom du périphérique cible. Cliquez ensuite sur **Paramètres** pour ouvrir la page de propriétés du périphérique. Cette page contient toutes les informations nécessaires.

Périphérique à bandes.

Si un périphérique à bandes est connecté à votre système, la syntaxe de l'adresse SCSI diffère selon que le pilote de bandes d'origine est chargé ou non. La syntaxe dépend également du système utilisé. Reportez-vous aux sections suivantes pour obtenir des instructions sur la création d'une adresse SCSI cible sur :

Windows sans le pilote de bandes d'origine

Windows avec pilote de bandes d'origine

Windows sans le pilote de bandes d'origine

Si le Disque de Bande Natif est déchargé, la syntaxe d'adresse SCSIest `P:B:T:L` (`P`=port SCSI, `B`=numéro Bus, `T`=ID Cible SCSI, `L`=LUN). Consultez les propriétés des lecteurs de bandes connectés pour collecter ces informations.

Ouvrez **Cartes SCSI** dans le **Panneau de configuration** et cliquez deux fois sur le nom du périphérique cible. Cliquez ensuite sur **Paramètres** pour ouvrir la page de propriétés du périphérique. Cette page contient toutes les informations nécessaires.

Windows avec pilote de bandes d'origine

Si le pilote de bandes d'origine est chargé, la syntaxe de l'adresse SCSI est `tapeN` (`N`=numéro d'instance du lecteur). Le fichier de lecteur de bandes ne peut être créé qu'à l'aide du nombre d'instances du lecteur, par exemple, `tape0` si `N` est égal à `0`.

Procédure

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**.
3. Cliquez sur le lecteur de bande avec le bouton droit de la souris, puis sélectionnez **Propriétés**.

   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.

Recherche de fichiers de périphérique sur un système UNIX

Pour configurer un périphérique connecté à un système UNIX, vous devez connaître les noms des fichiers de ce périphérique.

La création de fichiers de périphérique dépend du fournisseur du système d'exploitation UNIX spécifique. Pour les périphériques utilisés sur les plates-formes HP-UX et Solaris, reportez-vous aux sections ci-après. Pour les périphériques utilisés sur d'autres plates-formes UNIX, consultez les informations du fournisseur correspondant.

Recherche de fichiers de périphérique sur HP-UX

Conditions préalables

Vérifiez que le périphérique est correctement relié à l'aide de la commande `/usr/sbin/ioscan -f`.

Procédure

1. Sur votre système HP-UX, lancez l'application **System Administration Manager (SAM)**.
2. Cliquez sur **Périphériques**, puis sur **Lecteurs de bande**.
3. Cliquez sur le périphérique cible.
4. Dans le menu Actions, cliquez sur **ShowDevice Files**. Les noms des fichiers de périphérique s'affichent. Utilisez ceux dont la syntaxe est `*BEST`. Pour un périphérique sans rembobinage, utilisez la syntaxe `'BESTn'`.

Si aucun nom de fichier n'apparaît, vous devez créer les fichiers.

Recherche de fichiers de périphérique sur Solaris

Procédure

1. Appuyez sur **Stop** et **A** pour arrêter le système client.
2. A l'invite `ok`, utilisez la commande `probe-scsi-all` pour vérifier si le périphérique est

correctement connecté.

Vous obtenez des informations sur les périphériques SCSI connectés, y compris la chaîne ID du nouveau périphérique de sauvegarde.

3. A l'invite `ok`, entrez `go` pour reprendre l'exécution normale.
4. Affichez le contenu des répertoires `/drv/rmt` et, dans le cas d'une bibliothèque `/drv` :
   - Le répertoire `/drv/rmt` doit contenir le ou les noms de périphérique des lecteurs du périphérique de sauvegarde.
   - Le répertoire `/drv` doit contenir le nom de fichier de périphérique du robot, si vous utilisez un périphérique de bibliothèque multilecteur.

Si aucun nom de fichier n'apparaît, vous devez créer les fichiers.

Pour obtenir des informations détaillées sur les fichiers de périphérique, reportez-vous au *Guide d'installation HPE Data Protector*.

Création de fichiers de périphérique sur les systèmes UNIX

Si les fichiers de périphérique correspondant à un périphérique de sauvegarde particulier n'ont pas été créés lors de l'initialisation du système (processus de démarrage), vous devez les créer manuellement. Ce cas se présente avec les fichiers de périphériques requis pour gérer le périphérique de contrôle de bibliothèque (robots de bibliothèques).

La création de fichiers de périphérique dépend du fournisseur du système d'exploitation UNIX spécifique. Pour les périphériques utilisés sur les plates-formes HP-UX et Solaris, reportez-vous aux sections ci-après. Pour les périphériques utilisés sur d'autres plates-formes UNIX, consultez les informations du fournisseur correspondant.

Création de fichiers de périphérique sur les systèmes HP-UX

Conditions préalables

- Vérifiez que le périphérique est correctement relié à l'aide de la commande `/usr/sbin/ioscan -f`.

Procédure

1. Sur votre système HP-UX, lancez l'application **System Administration Manager (SAM)**.
2. Cliquez sur **Périphériques**, puis sur **Lecteurs de bande**.
3. Cliquez sur le périphérique cible.
4. Dans le menu Actions, cliquez sur **Create Device Files** puis sur **Create Default Device Files**.

Création de fichiers de périphérique sur les systèmes Solaris

Conditions préalables

- Avant de pouvoir utiliser un nouveau périphérique de sauvegarde sur un client Solaris, vous devez d'abord mettre à jour le périphérique et les fichiers de configuration du pilote pour le client, installer un autre pilote si vous utilisez un périphérique de bibliothèque, et créer de nouveaux fichiers périphérique sur le client.

Procédure

1. Appuyez sur **Stop** et **A** pour arrêter le système client.
2. A l'invite `ok`, exécutez la commande `probe-scsi-all` pour vérifier les adresses SCSI disponibles sur le système client, puis choisissez une adresse pour le périphérique que vous voulez connecter (pour un périphérique à un seul lecteur). Dans le cas d'un périphérique à plusieurs lecteurs, vous devrez choisir une adresse SCSI pour chaque lecteur et une pour le mécanisme du robot.
3. A l'invite `ok`, entrez `go` pour reprendre l'exécution normale.
4. Arrêtez et éteignez le système client.
5. Configurer la ou les adresses SCSI choisies sur le périphérique de sauvegarde.
6. Si nécessaire lors de la connexion de périphériques SCSI au système du client concerné, arrêtez et éteignez le système.
7. Connectez le périphérique de sauvegarde au système client
8. Allumez d'abord le périphérique de sauvegarde, puis le système client (s'il a été éteint auparavant).
9. Appuyez sur **Stop** et **A** pour arrêter de nouveau le système client.
10. À l'invite `ok`, naviguez vers `probe-scsi-all`.

    Vous obtenez des informations sur les périphériques SCSI connectés, y compris les chaînes ID correctes du nouveau périphérique de sauvegarde.
11. A l'invite `ok`, entrez `go` pour reprendre l'exécution normale.
12. Editez le fichier de configuration st.conf et ajouter les informations de périphérique et les adresses SCSI nécessaires pour les lecteurs.

    Pour plus d'informations sur cette opération, reportez-vous au document *Guide d'installation HPE Data Protector*.
13. Si vous connectez un périphériques multilecteurs avec un mécanisme de robot, effectuez également les étapes ci-dessous. Pour plus d'informations, reportez-vous à la section *Guide d'installation HPE Data Protector*.
    a. Copiez et installez un pilote `sst` sur le client.
    b. Copiez le fichier de configuration sst.conf (Solaris 8 ou 9) ou `sgen.conf` (Solaris 10) sur le système client concerné, éditez-le, puis ajoutez une entrée pour le mécanisme du robot.
    c. Éditez le fichier `/etc/devlink.tab` et ajoutez une entrée pour le fichier de périphérique du mécanisme de robot.
14. Lorsque vous avez mis à jour les pilotes et les fichiers de configuration selon vos besoins, créez

de nouveaux fichiers de périphérique pour le système client :

a. Supprimez tous les fichiers de périphérique existants du répertoire `/drv/mnt/`.
b. Exécutez la commande `shutdown -i0 -g0` pour éteindre le système.
c. Exécutez la commande `boot -rv` pour redémarrer le système.
d. Lorsque le redémarrage est terminé, affichez le contenu du répertoire `/dev` pour vérifier les fichiers de périphérique créés. Les fichiers de périphérique des mécanismes de robot devraient figurer dans le répertoire `/dev`, et ceux des lecteurs, dans le répertoire `/dev/rmt`.

Détection automatique des fichiers de périphérique et des adresses SCSI

Vous pouvez détecter automatiquement les noms de fichiers de périphérique (adresses SCSI) de la plupart des périphériques connectés aux plates-formes Windows, HP-UX ou Solaris.

Pour une définition de périphérique Data Protector existante

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**. La liste des périphériques configurés s'affiche dans la zone de résultats.
3. Dans la zone de résultats, cliquez avec le bouton droit sur le périphérique voulu puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet Lecteurs.
5. Sélectionnez dans la liste déroulante les adresses SCSI (noms de fichiers) du périphérique à détecter automatiquement.

Lors de la création d'une définition de périphérique Data Protector

Procédure

1. Suivez la procédure de configuration d'un périphérique.
2. Dans l'assistant, lorsqu'il vous est demandé de spécifier le nom du fichier de périphérique (adresse SCSI), utilisez la liste déroulante pour obtenir la liste des périphériques disponibles.

Détection automatique des fichiers de périphérique et des adresses SCSI pour les bibliothèques

Vous pouvez détecter automatiquement les fichiers de périphérique (adresses SCSI) des robots de bibliothèque connectés aux plates-formes Windows, HP-UX ou Solaris.

Pour une bibliothèque déjà configurée

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**. La liste des périphériques configurés s'affiche dans la zone de résultats.
3. Dans la zone de résultats, cliquez avec le bouton droit sur la bibliothèque voulue puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Contrôle**.
5. Dans la liste déroulante de la zone de l'adresse SCSI du robot de bibliothèque, vous trouverez les noms de fichiers disponibles (adresses SCSI) pour le robot de la bibliothèque.

Lors de la configuration d'une bibliothèque

Procédure

1. Suivez la procédure de configuration du robot de la bibliothèque.
2. Dans l'assistant, lorsqu'il vous est demandé de spécifier l'adresse SCSI (nom de fichier), utilisez la liste déroulante pour obtenir les noms de fichiers disponibles (adresses SCSI) pour le robot de la bibliothèque.

À propos de la configuration des périphériques de sauvegarde

Une fois la phase de préparation terminée, vous pouvez configurer un périphérique de sauvegarde à utiliser avec Data Protector.

Il est recommandé de laisser Data Protector configurer automatiquement les périphériques de sauvegarde. Data Protector peut automatiquement configurer les périphériques de sauvegarde les plus courants, notamment les bibliothèques. Vous devez toujours préparer le support pour une session de sauvegarde, mais Data Protector détermine le nom, la stratégie, le type de support, la stratégie de support et le fichier de périphérique ou l'adresse SCSI du périphérique, et configure le lecteur et les emplacements.

Vous pouvez également configurer manuellement un périphérique de sauvegarde. La configuration d'un périphérique de sauvegarde dépend de son type.

Vous pouvez utiliser des périphériques qui ne sont pas mentionnés comme étant pris en charge dans *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*. Les périphériques non pris en charge sont configurés à l'aide du fichier `scsitab`.

À propos de la Console de gestion de bibliothèque

Qu'est-ce qu'une console de gestion de bibliothèque ?

Parmi les bibliothèques de bandes actuelles, beaucoup sont fournies avec une console de gestion intégrée qui permet d'effectuer à distance des tâches de configuration, de gestion et de suivi de la bibliothèque. Une console de gestion de bibliothèque est une interface Web pour bibliothèque, qui se présente dans le navigateur Web comme une page Web ordinaire. Avec une bibliothèque de bandes équipée d'une console Web de ce type, vous pouvez exécuter diverses tâches depuis un système distant, quel qu'il soit. Par exemple, vous pouvez définir les paramètres de configuration de la bibliothèque, charger des bandes dans des lecteurs de la bibliothèque ou encore consulter l'état actuel de la bibliothèque. L'étendue des tâches pouvant être effectuées à distance dépend de l'implémentation de la console de gestion, laquelle est indépendante de Data Protector.

Chaque console de gestion de bibliothèque dispose de sa propre adresse URL (adresse Web), qui constitue le point d'entrée de l'interface de la console. Pour accéder à cette interface, entrez l'adresse URL dans la barre d'adresse d'un navigateur Web.

Prise en charge des consoles de gestion de bibliothèque dans Data Protector

La configuration de la bibliothèque contient un paramètre représentant l'URL de la console de gestion de bibliothèque. L'**URL de console de gestion** peut être indiquée pendant le processus de configuration ou de reconfiguration de la bibliothèque.

L'accès à l'interface de la console est simplifié par la fonction étendue d'interface utilisateur graphique de Data Protector. Vous pouvez ainsi appeler un navigateur Web et charger l'interface de la console depuis l'interface utilisateur graphique de Data Protector. Selon le système d'exploitation installé, c'est le navigateur Web par défaut du système (sous Windows) ou le navigateur Web défini dans la configuration de Data Protector (sous UNIX) qui est sollicité.

> **IMPORTANT :**
> Avant d'utiliser la console de gestion de bibliothèque, notez que certaines opérations exécutées par le biais de cette dernière peuvent interférer avec vos opérations de gestion des supports et/ou vos sessions de sauvegarde et de restauration.

Limite

L'adresse URL de la console de gestion ne doit pas contenir d'espaces ni de guillemets. Veillez à remplacer ces caractères par des codes URL standard. Le tableau ci-dessous récapitule les caractères non pris en charge et les codes URL équivalents.

Caractère	Code URL équivalent
Espace	%20
Guillemet (")	%22

Configuration automatique d'un périphérique de sauvegarde

Une fois que le périphérique de sauvegarde est connecté aux systèmes que vous souhaitez configurer et que les fichiers de périphérique de travail (adresse SCSI) existent, vous pouvez configurer le périphérique en vue de l'utiliser avec Data Protector. La configuration automatique implique que Data Protector crée une définition de périphérique.

Data Protector peut détecter et configurer automatiquement la plupart des périphériques de sauvegarde courants qui sont connectés à un ou à plusieurs systèmes dans un environnement SAN. Vous pouvez modifier ultérieurement les propriétés du périphérique configuré automatiquement, afin de l'adapter à vos besoins spécifiques.

La configuration automatique est possible sur les systèmes d'exploitation suivants :

- Windows
- HP-UX
- Solaris
- Linux

> **REMARQUE :**
> Si vous configurez automatiquement des bibliothèques alors que le service Gestionnaire de supports amovibles est actif, les lecteurs et les robots (échangeurs) ne seront pas combinés correctement.

Conditions préalables

Un Agent de support doit être installé sur chaque système client à configurer automatiquement.

Configuration automatique des périphériques

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Autoconfigurer périphériques** pour ouvrir l'assistant.
3. Sélectionnez le système client comportant les périphériques à configurer, puis cliquez sur **Suivant**.
4. Sélectionnez les périphériques de sauvegarde à configurer sur votre système. Cliquez sur **Suivant**.
5. Pour activer la détection automatique des adresses SCSI modifiées, sélectionnez l'option **Découvrir automatiquement adresse SCSI modifiée** et cliquez sur **Terminer**. Pour les périphériques de magasin, remplacez, une fois la configuration automatique terminée, le pool de supports par un pool avec support de magasin.

Le nom du périphérique s'affiche dans la liste de périphériques configurés. Vous pouvez analyser le périphérique pour en vérifier la configuration.

Configuration automatique des périphériques dans un environnement SAN

Data Protector fournit une fonction de configuration automatique des périphériques dans un environnement SAN où différents clients utilisent les lecteurs de bande d'une bibliothèque. Cette fonction de Data Protector permet de configurer automatiquement des périphériques et des bibliothèques sur plusieurs systèmes client.

Data Protector détermine le nom, le nom de verrouillage, la stratégie, le type de support, la stratégie de support, et le fichier de périphérique ou l'adresse SCSI du périphérique, et configure le lecteur et les emplacements.

> **REMARQUE :**
> Lorsque vous ajoutez un hôte dans un environnement SAN, les bibliothèques et les périphériques configurés ne sont pas mis à jour automatiquement.
>
> - Pour utiliser une bibliothèque existante sur un nouvel hôte, supprimez celle-ci et configurez-en automatiquement une nouvelle avec le même nom sur le nouvel hôte.
> - Pour ajouter des périphériques à une bibliothèque existante, vous pouvez supprimer la bibliothèque puis en configurer automatiquement une nouvelle avec le même nom et les nouveaux lecteurs sur un nouvel hôte ou ajouter manuellement les lecteurs à la bibliothèque.

Limites

La configuration automatique ne peut pas être utilisée pour configurer les périphériques suivants dans un environnement SAN :

- bibliothèques de supports mixtes,
- bibliothèques DAS ou ACSLS,
- périphériques NDMP.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Autoconfigurer périphériques** pour ouvrir l'assistant.
3. Sélectionnez les systèmes clients à configurer. Dans un environnement Microsoft Cluster Server, sélectionnez le serveur virtuel.

   Cliquez sur **Suivant**.
4. Sélectionnez les périphériques et les bibliothèques à configurer sur le système.
5. Dans le cas d'une bibliothèque, sélectionnez l'hôte de contrôle (client qui contrôle le robot de la bibliothèque lorsque celle-ci est visible par plusieurs clients). Si un Gestionnaire de cellule fait partie des systèmes qui voient la bibliothèque, il est sélectionné par défaut. Vous pouvez basculer entre les deux affichages suivants :

- **Regrouper par périphériques**

  Affiche la liste de l'ensemble des périphériques et bibliothèques. Développez le périphérique (ou la bibliothèque), et sélectionnez le système client sur lequel vous voulez le configurer.

- **Regrouper par hôtes**

  Affiche la liste des clients auxquels des périphériques sont connectés. Développez le client sur lequel vous souhaitez configurer des périphériques ou des bibliothèques.

6. Pour activer des périphériques MultiPath, vous pouvez également sélectionner l'option **Configurer automatiquement les périphériques MultiPath**. Cliquez sur **Suivant**.
7. Pour activer la détection automatique des adresses SCSI modifiées, sélectionnez l'option **Découvrir automatiquement adresse SCSI modifiée**.
8. Cliquez sur **Terminer**. La liste des périphériques configurés apparaît.

Vous pouvez analyser le périphérique pour en vérifier la configuration.

Configuration d'un périphérique autonome

Une fois que le périphérique de sauvegarde est connecté au système et qu'un fichier de périphérique de travail (adresse SCSI) existe, vous pouvez configurer le périphérique pour pouvoir l'utiliser avec Data Protector.

Il est recommandé de laisser Data Protector configurer automatiquement les périphériques de sauvegarde.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
3. Dans la zone de texte Nom de périphérique, saisissez le nom du périphérique.
4. Dans la zone de texte Description, vous pouvez saisir une description (facultatif).
5. Vous pouvez également sélectionner **Périphérique MultiPath**.
6. Si l'option **Périphérique MultiPath** n'est *pas* sélectionnée, sélectionnez le nom du client (système de sauvegarde) dans la liste déroulante Client.
7. Dans la liste Type de périphérique, sélectionnez le type de périphérique **Autonome**, puis cliquez sur **Suivant**.
8. Saisissez l'adresse SCSI du périphérique physique (systèmes Windows) ou un nom de fichier de périphérique (systèmes UNIX), cliquez sur **Ajouter.**

   Pour les périphériques MultiPath, sélectionnez le client dans la liste déroulante et saisissez le nom de fichier du périphérique. Cliquez sur **Ajouter** pour ajouter le chemin d'accès à la liste des chemins configurés.

   > **CONSEIL :**
   > Vous pouvez saisir plusieurs adresses pour créer une chaîne de périphériques.

> L'ordre d'ajout des périphériques à la chaîne détermine celui de leur utilisation par Data Protector.
>
> Lorsque tous les supports d'une chaîne de périphériques sont pleins, Data Protector émet une demande de montage. Remplacez le support du premier périphérique par un nouveau, formatez-le, puis confirmez la demande de montage. peut utiliser immédiatement les supports reconnus et non protégés. Data Protector peut immédiatement utiliser les supports reconnus et non protégés. Il est également possible d'utiliser un support vierge.

9. Sélectionnez **Découvrir automatiquement adresse SCSI modifiée** si vous souhaitez activer la découverte automatique d'adresses SCSI modifiées. Cliquez sur **Suivant**.
10. Dans la liste Type de support, sélectionnez un type de support pour le périphérique que vous êtes en train de configurer.
11. Indiquez un pool de supports pour le type de support sélectionné. Vous pouvez soit sélectionner un pool dans la liste déroulante Pool de supports, soit saisir un nouveau nom de pool. Dans ce cas, le pool sera créé automatiquement.
12. Cliquez sur **Terminer** pour quitter l'assistant.

Le nom du périphérique s'affiche dans la liste de périphériques configurés. Vous pouvez analyser le périphérique pour en vérifier la configuration. Si le périphérique est correctement configuré, Data Protector peut charger, lire et décharger des supports dans les emplacements.

Configuration d'une sauvegarde sur périphériques sur disque

Avant d'effectuer une sauvegarde à l'aide d'un périphérique sur disque (B2B), vous devez configurer le périphérique à utiliser avec Data Protector. La sauvegarde disponible vers les dispositifs de disque sont : le système de sauvegarde StoreOnce, le logiciel StoreOnce, Cloud (Helion), Cloud (Azure), Data Domain Boost et Smart Cache.

Prise en charge multi-interface

Data Protector offre une assistance multi-interface. Data Protector Prend en charge les connexions IP et Fiber Channel à la même banque Catalyst / DDBoost sans qu'il soit nécessaire de configurer une banque distincte. La banque est accessible simultanément via les deux interfaces.

Par exemple, une même banque Catalyst / DDBoost peut être accessible aux clients locaux via une connexion Fiber Channel pour une sauvegarde plus rapide alors que les clients distants ont accès à la même banque via un réseau WAN pour une sauvegarde plus lente.

Cette fonctionnalité n'est pas disponible dans l'environnement Solaris ou si la connexion FC est configurée comme identificateur pour la cible de déduplication. Cette option s'applique uniquement aux systèmes de sauvegarde StoreOnce et aux périphériques DD Boost.

Pour de plus amples détails sur le fonctionnement de cette caractéristique, consultez le *Guide de l'Administrateur de Data Protector HPE* , et*Guide de référence de l'interface de ligne de commande HPE Data Protector*.

> **IMPORTANT :**
> Il est fortement recommandé d'utiliser une adresse IP ou un nom d'hôte lors de l'ajout de

périphériques StoreOnce ou DDBoost afin de profiter de la fonctionnalité multi interface.

Procédure

Pour ajouter un dispositif B2D (qui cible un stockage existant), procédez de la manière suivante :

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
3. Indiquez le nom du périphérique et une description (facultatif).
4. Sélectionnez le type de dispositif **Sauvegarde vers Disque** puis sélectionnez le **Type d'Interface** : **Système de Sauvegarde StoreOnce**, **Data Domain Boost**, **Logiciel StoreOnce** , **Cloud (Helion)**, **Cloud (Azure)** ou **Smart Cache**.
5. Les étapes pour configurer le périphérique varient en fonction du type d'interface sélectionné.
   - Configuration de StoreOnce
   - Configuration du Logiciel StoreOnce
   - Configuration de Data Domain Boost
   - Configuration de Smart Cache
   - Configuration des périphériques cloud (Helion)
   - Configuration des périphériques cloud (Azure)

La procédure pour ajouter un dispositif B2D est similaire à la procédure pour ajouter des types de dispositif. De plus, pour les dispositifs de déduplication du Logiciel StoreOnce, vous devez d'abord configurer un répertoire root puis créer un stockage (consultez Configuration d'un périphérique de sauvegarde sur disque - Logiciel StoreOnce).

Configuration d'un périphérique de sauvegarde sur disque - StoreOnce

Avant d'effectuer une sauvegarde à l'aide d'un périphérique sur disque (B2B), vous devez configurer le périphérique à utiliser avec Data Protector.

Si vous configurez un périphérique de déduplication du logiciel StoreOnce, des étapes supplémentaires sont nécessaires. Consultez Configuration d'un périphérique de sauvegarde sur disque - Logiciel StoreOnce.

REMARQUE :
HPE Data Protector prend en charge les banques fédérées contenant jusqu'à huit membres. Le nombre de membres d'une banque peut être modifié dans StoreOnce. Pour refléter ce changement, vous pouvez actualiser manuellement le cache HPE Data Protector dans l'interface utilisateur graphique ou l'interface de ligne de commande HPE Data Protector. Pour plus d'informations, voir Actualisation du cache pour les banques. Tous les membres de la fédération doivent être en ligne pour qu'une banque fédérée fonctionne.

Procédure

Pour ajouter un système de sauvegarde StoreOnce ou un périphérique B2D logiciel StoreOnce (qui cible une banque existante), procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
3. Indiquez le nom du périphérique et une description (facultatif).
4. Sélectionnez le type de périphérique **Sauvegarde sur disque**, puis le Type d'interface : **Système de sauvegarde StoreOnce** ou **Logiciel StoreOnce**.
5. Dans la zone de texte relative à l'adresse **URL de la console de gestion**, entrez une URL valide pour la console de gestion de périphérique (facultatif). Cliquez sur **Suivant**.
6. Pour les périphériques d'un système StoreOnce Backup, entrez l'**ID client** et éventuellement le mot de passe pour accéder à la banque. Vous pouvez utiliser les caractères suivants pour le mot de passe : [a-z][A-Z][0-9][_-.+(){}:#$*;=?@[]^|~]?
7. Dans le champ **Système de déduplication**, entrez le nom d'hôte, l'adresse IP, le nom de domaine complet (FQDN) ou l'adresse Fiber Channel (FC) du système de déduplication (la machine qui héberge la banque de déduplication).

   Ou cliquez sur **Sélectionner le jeu de services** pour interroger et retrouver l'adresse du système de d&éduplication.

   > **REMARQUE :**
   > Pour l'interface StoreOnce Software, seuls une adresse IPv4 ou IPv6 et un nom de domaine complet sont pris en charge. Cependant, pour l'interface du système StoreOnce Backup, une adresse IPv4 ou IPv6, un nom de domaine complet ou un identifiant global FC sont pris en charge, à condition d'utiliser la dernière version de StoreOnce Catalyst.
   >
   > Si vous vous connectez au périphérique d'un système StoreOnce Backup à l'aide de FC, spécifiez l'adresse FC du périphérique. Assurez-vous d'utiliser des Agents de support ou des passerelles connectés au périphérique FC et qu'ils figurent dans la même zone que le périphérique du système StoreOnce Backup.

8. Cliquez sur le bouton **Sélectionner/créer une banque** pour sélectionner une banque fédérée ou non fédérée existante ou pour créer une banque non fédérée. Sélectionnez le nom de la banque dans la liste.

   Pour créer une banque cryptée, sélectionnez l'option **Banque cryptée**. Cliquez sur **OK**.

   > **REMARQUE :** Le chiffrement ne peut être activé qu'au moment de la création de la banque. Une fois la banque créée, elle ne peut plus être convertie de l'état crypté à l'état non crypté, ou vice versa. Les services de déduplication du logiciel StoreOnce ne prennent pas en charge le chiffrement des banques.
   > Vous ne pouvez pas créer une banque fédérée en utilisant l'interface graphique Data Protector. Vous devez les créer en utilisant la console de gestion StoreOnce.

9. Vous pouvez également sélectionner l'option **Déduplication côté source** pour activer la déduplication côté source. La fenêtre des propriétés de déduplication côté source s'affiche. Vérifiez et modifiez les propriétés si nécessaire. Par défaut, la passerelle côté source s'appelle

`DeviceName_Source_side`. Notez que vous ne pouvez créer qu'une seule passerelle côté source par périphérique. Cette passerelle (virtuelle) sera alors automatiquement étendue sur le système sauvegardé si la déduplication côté source est activée dans la spécification de sauvegarde.

> **REMARQUE :**
> Pour les banques fédérées, toutes les opérations d'écriture sont effectuées en mode bande passante faible (déduplication côté serveur). Même si une passerelle est configurée comme déduplication côté cible (mode bande passante large), le passage se fait automatiquement vers le mode bande passante étroite.

10. Sélectionnez une passerelle et cliquez sur **Ajouter** pour afficher la boîte de dialogue des propriétés. Si nécessaire, modifiez les propriétés de la passerelle puis cliquez sur **OK** pour l'ajouter. Si vous vous connectez au système StoreOnceBackup à l'aide de FC, assurez-vous d'utiliser des Agents de support ou des passerelles connectés au périphérique FC et qu'ils figurent dans la même zone que le périphérique du système StoreOnce Backup.

    > **REMARQUE :**
    > Le membre de la fédération connecté à la passerelle HPE Data Protector doit être membre de la banque fédérée. Si le membre de la fédération est détaché à l'aide de StoreOnce, ajustez la passerelle HPE Data Protector afin de l'attacher à un autre membre de la fédération en suivant les étapes de la section Actualisation du cache pour les banques.

    Pour afficher les propriétés de la passerelle, sélectionnez la passerelle souhaitée puis cliquez sur **Propriétés**. Pour définir des options de passerelle supplémentaires, cliquez dans l'onglet **Paramètres** puis sélectionnez **Avancé** pour ouvrir la fenêtre des propriétés avancées.

    Dans la fenêtre Propriétés avancées, pour limiter le nombre de flux sur chaque passerelle, sélectionnez **. Nombre de flux parallèles par passerelle**. Vous pouvez spécifier un maximum de 100 flux. Si vous ne sélectionnez pas cette option, le nombre de flux n'est pas limité. Notez que vous pouvez également configurer cette option lors de la création d'une spécification de sauvegarde. Dans ce cas, la valeur spécifiée lors de la création d'un périphérique B2D sera écrasée.

    Pour limiter la bande passante réseau utilisée par la passerelle, sélectionnez **Limite de bande passante réseau de passerelle (Kbps)** et entrez la limite en kilobits par seconde (Kbps).

    Pour activer la déduplication côté serveur, sélectionnez **Déduplication côté serveur**.

    Si vous avez configuré une adresse IP ou un FQDN comme cible de déduplication, les options **Utiliser FC** et **Reprise sur IP** sont disponibles et sélectionnées par défaut.

11. Pour vérifier la connexion, cliquez sur **Vérifier**.
12. Cliquez sur **Suivant** pour passer à la fenêtre Paramètres, dans laquelle vous pouvez spécifier les options suivantes :
    - Max. Nombre de connexions par banque
    - Quota logiciel de la taille de la sauvegarde (Go)
    - Quota logiciel de la taille de la banque (Go)
    - **Taille de seuil d'élément Catalyst (Go)** : Définit la taille de seuil de l'élément Catalyst pour la déduplication logicielle StoreOnce et pour les périphériques du système StoreOnce Backup. Lorsque cette taille est dépassée, les objets ne seront plus ajoutés à l'élément Catalyst actuel.

Par défaut, la taille de l'élément Catalyst est illimitée.

- **Objet unique par élément Catalyst** : Sélectionnez cette option pour autoriser un objet par élément Catalyst pour la déduplication logicielle StoreOnce et pour les périphériques du système StoreOnce Backup.

13. Cliquez sur **Suivant** pour afficher la fenêtre Résumé, qui affiche des détails sur la banque B2D configurée. En outre, pour une banque fédérée, elle inclut une liste de tous les membres de la fédération et leur statut (en ligne ou hors ligne).
14. Vérifiez les paramètres et cliquez sur **Terminer**. Le nouveau périphérique B2D configuré apparaît dans la fenêtre de navigation.

Actualisation du cache pour les magasins

StoreOnce 3.12 vous permet d'ajouter ou de supprimer certains membres de fédération de banques fédérées. Pour refléter ce changement, vous pouvez actualiser manuellement le cache HPE Data Protector dans l'interface utilisateur graphique ou l'interface de ligne de commande HPE Data Protector.

Actualisation du cache à l'aide de l'interface graphique de HPE Data Protector

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Périphériques**.
3. Cliquez avec le bouton droit de la souris sur le périphérique StoreOnce souhaité, puis sélectionnez **Propriétés**.
4. Cliquez dans l'onglet **Banque et passerelles**, puis cliquez sur **Sélectionner/créer une banque**. Si nécessaire, modifiez le chemin du répertoire pour inclure l'adresse d'un membre actif de la fédération.
5. Sélectionnez la même banque, qui est associée à ce périphérique StoreOnce, puis cliquez sur **OK**.
6. Cliquez sur **Appliquer**.

Actualisation du cache à l'aide de l'interface de ligne de commande de HPE Data Protector

1. Exécutez la commande suivante :

   ```
   omnidownload –library <NomPériphériqueDP> -file
   <FichierSortiePériphériqueDP>
   ```

2. Éditez `FichierSortiePériphériqueDP`.

   Si le périphérique n'est pas fédéré, supprimez les lignes suivantes :

   ```
   B2DTEAMEDSTORE 1
   B2DTEAMEDMEMBERS
   "<teamed.device.one>"
   "<teamed.device.two>"
   ...
   ```

Si le périphérique est fédéré, ajoutez ces lignes à `FichierSortiePériphériqueDP` après avoir remplacé les adresses IP du périphérique associé approprié. Si nécessaire, modifiez le chemin du répertoire pour inclure l'adresse d'un membre actif de la fédération.

> **REMARQUE : Remarque :** les adresses et le format doivent correspondre exactement à ceux du fichier de stratégie d'association StoreOnce. Par exemple, si le fichier de stratégie d'association inclut une adresse IPv6, vous devez également ajouter la même adresse à ce fichier.

3. Enregistrez le fichier modifié en utilisant la commande suivante :

   ```
   omniupload –modify_library <NomPériphériqueDP> -file
   <FichierSortiePériphériqueDP>
   ```

Pour plus d'informations sur ces commandes, reportez-vous au *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Configuration d'un périphérique de sauvegarde sur disque - Logiciel StoreOnce

Si vous configurez un périphérique de déduplication du logiciel StoreOnce, des étapes supplémentaires sont nécessaires.

- Configuration du répertoire racine des banques de déduplication
- Création d'une banque

Configuration du répertoire racine des banques de déduplication

Cette section décrit la façon de configurer le répertoire racine des banques. Cette configuration doit être effectuée après l'installation du logiciel et avant de créer la première banque de déduplication.

Un même système de déduplication du logiciel StoreOnce peut servir d'hôte à plusieurs banques de déduplication, pourvu que les banques ne partagent pas un même répertoire racine. Chaque banque fonctionne indépendamment des autres, c'est-à-dire que la déduplication n'intervient qu'au sein d'une banque, et que chaque banque possède sa propre table d'index. Bien que toutes les banques fonctionnent selon le même processus, chacune peut être démarrée / arrêtée individuellement (cela ne signifie pas qu'une banque démarre / s'arrête physiquement, voir *Déduplication, livre blanc - Annexe A : utilitaire StoreOnceSoftware* pour plus de détails). Aucune opération ne peut être effectuée sur une banque si elle est arrêtée (hors ligne).

Des banques partageant le même répertoire racine ne peuvent être physiquement séparées. Cette conception garantit un chargement uniforme sur tous les disques et permet de meilleures performances.

Suite à une installation réussie, l'utilitaire StoreOnceSoftware démarre dans un mode où il s'exécute, mais attend la configuration du répertoire racine des banques. Aucun périphérique B2D ne peut être ajouté, et aucune banque ne peut être créée tant que le répertoire racine n'a pas été configuré.

Le répertoire racine des banques peut être configuré depuis :

- L'interface utilisateur graphique (GUI) : suivez la procédure pour l'ajout d'un périphérique, et spécifiez le répertoire racine lorsqu'on vous le demande (voir ci-dessous pour plus de détails).

- L'interface en lignes de commande (CLI) : utilisez la commande StoreOnceSoftware --configure_ store_root (voir *Déduplication, livre blanc - Annexe A : utilitaire StoreOnceSoftware* pour plus de détails).

> **REMARQUE :** Le répertoire racine doit déjà exister (sur le serveur), et vous devez disposer des accès en écriture pour pouvoir le configurer. En effet, le processus de configuration (GUI) vous demande de spécifier son emplacement.

La procédure de configuration du répertoire racine à l'aide de l'interface utilisateur graphique est similaire à la création d'une banque, mais comporte quelques étapes supplémentaires. Une fois la configuration du répertoire racine effectuée, ces étapes supplémentaires ne sont plus nécessaires. Pour configurer le répertoire racine (et créer une banque en même temps), réalisez les étapes suivantes :

1. Suivez la procédure d'ajout de périphérique :
   a. Dans le contexte Périphériques et supports, cliquez avec le bouton droit de la souris sur **Périphériques** > **Ajouter périphérique**.
   b. Spécifiez un nom de périphérique, ajoutez une description, sélectionnez le type de périphérique **Sauvegarde sur disque** et sélectionnez l'interface **Déduplication du logiciel StoreOnce**.
   c. Vous pouvez, si vous le souhaitez, saisir une URL valide de la console de gestion du périphérique dans la zone de texte URL de la **console de gestion**.
   d. Cliquez sur **Suivant** pour afficher l'écran dans lequel vous spécifiez une banque et une liste de passerelles.
   e. Pour les périphériques de système de sauvegarde StoreOnce, saisissez l'**ID client**, et éventuellement le **mot de passe** pour accéder à la banque.
2. Dans la case Système de déduplication, saisissez le nom d'hôte, l'adresse IP, ou le nom de domaine complet (FQDN) de la machine qui héberge la banque de déduplication).
3. Sélectionnez une passerelle, cliquez sur **Ajouter** pour afficher la boîte de dialogue des propriétés, puis cliquez sur **OK** pour ajouter la passerelle.
4. Cliquez sur **Vérifier**. Le message Répertoire racine non configuré s'affiche.
5. Dans la boîte de dialogue, spécifiez le chemin du répertoire racine (par exemple, C:\Volumes\StoreOnceRoot) qui doit héberger toutes les banques et cliquez sur **OK**. (remarque : il est impossible de parcourir les disques pour atteindre le répertoire racine valide).
6. Si le répertoire racine existe, la boîte de dialogue se ferme et la configuration du périphérique continue. L'utilitaire StoreOnceSoftware crée un sous-répertoire (la banque) dans le répertoire racine spécifié. Si le répertoire racine n'existe pas, un message d'erreur s'affiche.
7. Poursuivez avec la procédure d'ajout de périphérique.

Veuillez noter les points suivants lors de la configuration du répertoire racine et la création des banques :

- N'utilisez pas le même disque que celui où est installé le système d'exploitation (OS).
- Utilisez des disques de stockage dédiés (exclusivement).
- Data Protector prend en charge un maximum de 32 banques par volume.

> **REMARQUE :** Sur les systèmes Windows, pour améliorer les performances, appliquez les options suivantes au volume NTFS qui héberge les racines des banques.
> Désactivez la création de noms de fichiers courts (type DOS) sur le volume avec la commande

> : `fsutil behavior set Disable8dot3 Volume 1`
> Augmentez la taille des fichiers journaux internes NTFS avec la commande : `Chkdsk Volume /L:131072`

Création d'une banque

Avant de créer une banque, vérifiez que le répertoire racine des banques a été configuré et que les disques de stockage physiques (périphériques LUN) sont formatés et montés sur le système de déduplication du logiciel StoreOnce. Les périphériques LUN peuvent être sur des disques locaux ou des baies de disques (interface SCSI ou Fiber Channel), ou sur un périphérique NAS situé sur le même LAN (interface iSCSI). Si vous utilisez l'interface iSCSI, la connexion réseau fiable doit fournir une latence maximale de 2 ms et un débit minimal de 1 Gbit/s.

Une banque peut être créée depuis :

- L'interface utilisateur graphique : suivez la procédure pour l'ajout d'un périphérique, et spécifiez le nom de la banque lorsqu'on vous le demande (voir ci-dessous pour plus de détails).
- L'interface en lignes de commande (CLI) : utilisez la commande StoreOnceSoftware --create_store (voir *Déduplication, livre blanc - Annexe A : utilitaire StoreOnceSoftware* pour plus de détails).

La procédure de création d'une banque est similaire à l'ajout d'un périphérique, mais comprend quelques étapes supplémentaires. Pour créer une banque, procédez comme suit :

1. Suivez la procédure d'ajout de périphérique :
   a. Dans le contexte Périphériques et supports, cliquez avec le bouton droit de la souris sur **Périphériques** > **Ajouter périphérique**.
   b. Spécifiez un nom de périphérique, ajoutez une description, sélectionnez le type de périphérique **Sauvegarde sur disque** et sélectionnez l'interface **Déduplication du logiciel StoreOnce**.
   c. Cliquez sur **Suivant** pour afficher l'écran dans lequel vous spécifiez une banque et une liste de passerelles.
2. Sélectionnez le système de déduplication et spécifiez un nom pour la banque. La longueur maximale du nom de la banque est de 80 caractères (uniquement alphanumériques).
   a. Sélectionnez une passerelle, cliquez sur **Ajouter** pour afficher la boîte de dialogue des propriétés, puis cliquez sur **OK** pour ajouter la passerelle.
   b. Cliquez sur **Vérifier** pour vérifier la connexion. Si la banque n'existe pas encore, elle est créée. (Remarque : cliquer sur **Suivant** vérifiera également la connexion.)
   c. Poursuivez avec la procédure d'ajout de périphérique.

Si vous spécifiez un nom de banque incorrect, il est impossible de le modifier via l'interface utilisateur graphique. Vous devez relancer la procédure et créer la banque avec le bon nom. Utilisez l'interface en lignes de commande pour supprimer la banque au nom incorrect (à supposer qu'aucune donnée n'y a été écrite).

Configuration d'une sauvegarde sur périphérique sur disque - Data Domain Boost

Avant d'effectuer une sauvegarde à l'aide d'un périphérique sur disque (B2B), vous devez configurer le périphérique à utiliser avec Data Protector.

Conditions préalables

- Pour prendre en charge la réplication entre les périphériques de domaine de données, vous devez activer la synthèse virtuelle sur les périphériques de domaine de données.
  - Avec `ssh`, connectez-vous aux périphériques de domaine de données et exécutez la commande suivante :

    ```
    ddboost option set virtual-synthetics enabled
    ```

- Pour prendre en charge la réplication, le même utilisateur Data Domain Boost doit être configuré sur les périphériques source et cible avec le même rôle administratif. Pour plus d'informations, voir la documentation Data Domain.

Limites

- Lors d'une réplication interactive, une seule session peut être sélectionnée pour la réplication.
- Les opérations de Data Protector ne sont pas prises en charge lorsque la valeur par défaut du paramètre de puissance de cryptage est modifiée.

> **REMARQUE :** Dans le cas des périphériques d'amélioration du domaine de données, le terme « unité de stockage » est utilisé à la place du terme « banque ».

Procédure

Pour ajouter un périphérique DDBoost B2D (qui cible une banque existante), procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
3. Indiquez le nom du périphérique et une description (facultatif).
4. Sélectionnez le type de périphérique **Sauvegarde sur disque**, puis le **Type d'interface** : **Amélioration du domaine de données**.
5. Dans la zone de texte relative à l'adresse **URL de la console de gestion**, entrez une URL valide pour la console de gestion de périphérique (facultatif). Cliquez sur **Suivant**.
6. Entrez un **nom d'utilisateur** et un **mot de passe**. Vous pouvez utiliser les caractères suivants pour le mot de passe : [a-z][A-Z][0-9][_-.+(){}:#$*;=?@[]^|~]?
7. Entrez le nom de l'unité de stockage (ceci implique qu'il existe déjà).
8. Dans la zone de texte **Système de déduplication**, entrez le nom d'hôte, l'adresse IP ou l'adresse FC du système de déduplication (la machine d'hébergement où se trouve l'unité de stockage de déduplication).

   > **REMARQUE :** Il est recommandé d'utiliser l'adresse IP ou le FQDN pour tirer parti de la fonction multi-interface. Pour comprendre en quoi consiste cette fonction, reportez-vous à Prise en charge multi-interface.

9. Vous pouvez également sélectionner l'option **Déduplication côté source** pour activer la déduplication côté source. La fenêtre des propriétés de déduplication côté source s'affiche.

Vérifiez et modifiez les propriétés si nécessaire. Par défaut, la passerelle côté source s'appelle `DeviceName_Source_side`. Notez que vous ne pouvez créer qu'une seule passerelle côté source par périphérique. Cette passerelle (virtuelle) sera alors automatiquement étendue sur le système sauvegardé si la déduplication côté source est activée dans la spécification de sauvegarde.

10. Sélectionnez une passerelle et cliquez sur **Ajouter** pour afficher la boîte de dialogue des propriétés. Si nécessaire, modifiez les propriétés de la passerelle puis cliquez sur **OK** pour l'ajouter.

    Pour afficher les propriétés de la passerelle, sélectionnez la passerelle souhaitée puis cliquez sur **Propriétés**. Pour définir des options de passerelle supplémentaires, cliquez dans l'onglet **Paramètres** puis sélectionnez **Avancé** pour ouvrir la fenêtre des propriétés avancées.

    Pour limiter le nombre de flux sur chaque passerelle, sélectionnez **Max. Nombre de flux parallèles par passerelle**. Vous pouvez spécifier un maximum de 100 flux. Si vous ne sélectionnez pas cette option, le nombre de flux n'est pas limité. Notez que vous pouvez également configurer cette option lors de la création d'une spécification de sauvegarde. Dans ce cas, la valeur spécifiée lors de la création d'un périphérique B2D sera écrasée.

    Pour limiter la bande passante réseau utilisée par la passerelle, sélectionnez **Limite de bande passante réseau de passerelle (Kbps)** et entrez la limite en kilobits par seconde (Kbps).

    Si vous avez configuré une adresse IP ou un FQDN comme cible de déduplication, les options **Utiliser FC** et **Reprise sur IP** sont disponibles et sélectionnées par défaut.

    Pour activer la déduplication côté serveur, sélectionnez **Déduplication côté serveur**.

11. Pour vérifier la connexion, cliquez sur **Vérifier**.
12. Cliquez sur **Suivant** pour passer à la fenêtre Paramètres, dans laquelle vous pouvez spécifier les options suivantes :
    - **Nombre max. de connexions par unité de stockage :** Définit la médiane des limites maximum de flux en lecture et écriture de la connexion physique.
    - **Quota logiciel de la taille de la sauvegarde (Go) :** Entrez le quota logiciel de la taille de la sauvegarde (en Go)
    - **Quota logiciel de la taille de la banque (Go) :** Pris en charge si une unité de stockage est créée ou si les quotas sont manuellement activés pour le système DD OS (Data Domain Operating System) entier et spécifié lorsque l'unité de stockage est créée.
    - **Seuil de taille de support de banque (Go)** : Définit le seuil de taille de support de banque pour les périphériques d'amélioration du domaine de données. Lorsque cette taille est dépassée, les objets ne seront plus ajoutés à l'élément de banque actuel. Par défaut, la taille de l'élément de banque est illimitée.
    - **Objet unique par support de banque** : Sélectionnez cette option afin d'activer un objet par support de banque pour les périphériques d'amélioration du domaine de données.
13. Cliquez sur **Suivant** pour afficher la fenêtre Résumé, qui inclut des détails sur l'unité de stockage B2D configurée.
14. Vérifiez les paramètres et cliquez sur **Terminer**. Le nouveau périphérique B2D configuré apparaît dans la fenêtre de navigation.

Configuration de l'amélioration du domaine de données sur les systèmes AIX

Pour configurer l'amélioration du domaine de données via le protocole Fibre Channel (FC) sur les systèmes AIX, vous devez installer le pilote de périphérique AIX DDdfc. Le nom du fichier de pilote est DDdfc.1.0.0.x.bff, x correspondant au numéro de version.

Procédure

1. Connectez-vous au client AIX en tant qu'utilisateur root.
2. Entrez la commande `# smitty install`.
3. Sélectionnez **Installer et mettre à jour un logiciel**.
4. Sélectionnez **Installer un logiciel**.
5. Entrez le chemin d'accès `/usr/omni/drv` pour installer le fichier DDdfc.1.0.0.x.bff, x correspondant au numéro de version.
6. Appuyez sur **F4** pour sélectionner la version DDdfc.1.0.0.x que vous voulez installer.
7. Appuyez sur **Tab** pour faire basculer la valeur sur la ligne Aperçu uniquement ? sur Non.
8. Appuyez sur **Entrée** pour accepter les informations et installer le pilote.

Configuration d'une sauvegarde sur périphérique sur disque - Smart Cache

Avant d'effectuer une sauvegarde à l'aide d'un périphérique sur disque (B2B), vous devez configurer le périphérique à utiliser avec Data Protector.

Configuration de Smart Cache

Conditions préalables

- Vous devez disposer des identifiants utilisateur de l'hôte Agent de support sur lequel vous souhaitez créer le périphérique Smart Cache. Le plug-in VMware utilise ces identifiants pour accéder au partage réseau lors de la récupération sans étapes.

  > **REMARQUE :** Dans un hôte Agent de support, un seul identifiant utilisateur de système d'exploitation doit être utilisé pour créer un périphérique Smart Cache. Si plusieurs utilisateurs créent simultanément des périphériques Smart Cache sur le même hôte Agent de support, les demandes de restauration granulaire VMware peuvent rencontrer des erreurs de type "Accès refusé".

- Pour le système d'exploitation Linux, vous devez installer et exécuter le serveur Samba sur le client Smart Cache, car Data Protector utilise le serveur Samba pour créer des partages lors de la récupération. Pour vérifier que le serveur Samba est en cours d'exécution, exécutez la commande suivante `ps -ef | grep smbd`. Le mode de sécurité par défaut pour le serveur Samba est *user-level*. Si le mode par défaut est modifié, vous devez le mettre à jour à l'état *user-level* à l'aide de la commande suivante : `[global] security = user`.
- Vérifiez que les partages Samba disposent des autorisations en lecture-écriture. Si le module de

sécurité du noyau Security-Enhanced Linux (SELinux) est déployé dans votre système Linux, exécutez la commande `# setsebool -P samba_export_all_rw on` afin d'activer les autorisations de lecture-écriture pour les partages Samba.

- Sur le serveur Samba, vous devez ajouter l'utilisateur de l'hôte Agent de support pour 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`
- Vous devez effectuer un nettoyage régulier du fichier de configuration Samba, (smb.conf). Cela garantit la suppression des précédentes informations de configuration du partage Samba.
- Vous devez déployer l'agent de récupération VMware sans étapes et le module Agent de support sur le même hôte si le stockage Smart Cache est un système de fichiers Windows ReFS, un CIFS ou un partage NFS.
- Si le stockage Smart Cache est un disque fixe local ou un LUN de stockage SAN, l'hôte Agent de récupération VMware sans étapes et le module Agent de support peuvent être différents.
- Vous devez dédier la totalité du système de fichiers à un périphérique Smart Cache. Ce système de fichier ne doit pas être utilisé par d'autres applications et ne doit pas être partagé par d'autres périphériques Smart Cache ou de sauvegarde sur disque.
- Un seul pool de supports unique peut être associé à un périphérique Smart Cache.

Limites

- Smart Cache est disponible uniquement sur les plates-formes Windows x64 et Linux x64.
- Pour un périphérique Smart Cache Window situé sur un partage réseau, la GRE sans étapes est uniquement prise en charge sous Windows Server 2008 et les systèmes ultérieurs.
- Smart Cache est disponible comme cible de sauvegardes VMware uniquement.
- Sur les systèmes d'exploitation Linux, la sauvegarde sur Smart Cache n'est pas prise en charge si le paquet Agent de support NDMP est installé.
- Les sauvegardes VMware codées ou chiffrées AES 256 bits sur un périphérique Smart Cache ne sont pas prises en charge.
- La copie d'objet codée ou cryptée AES 256 bits d'une source sur un périphérique Smart Cache n'est pas prise en charge. Cependant, les copies d'objets depuis et vers des périphériques à bande dotés d'un cryptage matériel sont prises en charge.
- Un seul point de montage par périphérique Smart Cache est pris en charge.
- Le périphérique de sauvegarde sur Smart Cache risque d'échouer si l'espace est insuffisant. Assurez-vous qu'il y a suffisamment d'espace disque disponible sur le périphérique Smart Cache.
- L'exportation et l'importation de supports ne sont pas prises en charge par le périphérique Smart Cache.
- Si vous créez un périphérique Smart Cache sur un volume Resilient File System (ReFS) ou sur un partage réseau (CIFS/NFS), installez le composant proxy de montage (utilisé pour la récupération) sur le même hôte. Sinon, les récupérations avec étapes échoueront.
- CIFS n'est pas pris en charge avec la configuration des périphériques Smart Cache sur StoreOnce 4500.

Procédure

1. Créez un répertoire pour le périphérique Smart Cache dans l'emplacement requis sur le disque, par exemple, `c:\SmartCache`.

   Vous pouvez créer un périphérique Smart Cache sur un disque local ou réseau (ou sur un système de fichiers NFS monté pour les systèmes Linux). Pour spécifier un lecteur réseau, utilisez le format suivant : `\\hostname\share_name`.

   Les noms d'hôtes et leurs noms de partages ainsi que les lecteurs réseau n'apparaissent pas dans la boîte de dialogue Explorer lecteurs. Vous devez entrer le chemin vers les noms UNC.
2. Sur le système d'exploitation **Windows**, pour obtenir les autorisations d'accès au disque partagé contenant un périphérique Smart Cache, modifiez le compte Inet Data Protector sur l'Agent de support. Pour cela, fournissez des autorisations d'accès au système client local et aux disques partagés distants. En outre, assurez-vous qu'il s'agit d'un compte utilisateur spécifique, et non d'un compte système. Après avoir configuré le compte Inet, configurez et utilisez les périphériques Smart Cache sur des disques partagés.
3. Dans la liste de contexte de Data Protector, cliquez sur **Périphériques et supports**.
4. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
5. Indiquez le nom du périphérique et une description (facultatif).
6. Sélectionnez le type de périphérique **Sauvegarde sur disque**, puis le type d'interface **Smart Cache** :
7. Dans la liste déroulante Client, sélectionnez le système client sur lequel résidera le périphérique. Cliquez sur **Suivant**.
8. Entrez le nom d'utilisateur et le mot de passe de l'utilisateur qui a besoin d'accéder au partage créé pendant la récupération sans étapes.
9. Spécifiez un répertoire pour le périphérique Smart Cache. Cliquez sur **Ajouter**.
10. Pour afficher les propriétés par défaut d'un répertoire, sélectionnez le répertoire puis cliquez sur **Propriétés**.
11. Cliquez sur **Suivant** pour afficher la fenêtre Résumé. Vérifiez les paramètres et cliquez sur **Terminer**. Le nouveau périphérique B2D configuré apparaît dans la fenêtre de navigation.

Configuration des périphériques cloud (Helion)

Configurez un Cloud Helion device en préparation pour effectuer des copies d'objet vers le stockage d'objet Cloud.

En préparation, exécutez la procédure suivante :

- Obtention du nom du projet du cloud public HPE
- Obtention de l'URL du service d'authentification
- Créer des Clés d'Accès

Ensuite, vous pouvez configurer un dispositif de Cloud (Helion) comme sauvegarde vers le disque dur, dans Data Protector.

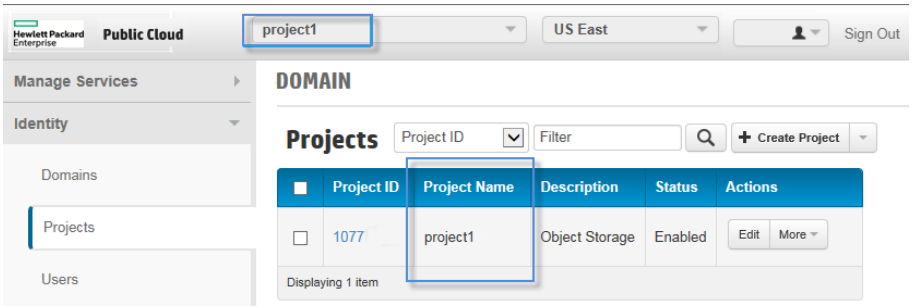
Configuration d'un périphérique de sauvegarde sur disque - Cloud (Helion)

Obtention du nom du projet du cloud public HPE

Procédure

1. Connectez-vous au HPE Public Cloud Console (https://horizon.hpcloud.com) avec vos codes d'accès HPE Public Cloud.
2. Sélectionnez le projet correspondant dans la liste des projets.
3. Notez le nom du projet afin de l'utiliser ultérieurement dans l'interface graphique de HPE Data Protector. Cela sera indiqué dans le champ Preneur/ Projet pendant la création du dispositif.

   Projet dans HPE Public Cloud



Obtention de l'URL du service d'authentification

Procédure

1. Dans le menu Utilisateur, sélectionnez **Roles and API Endpoints**. La page User Roles and API Endpoints s'ouvre.
2. Cliquez dans l'onglet **Service API Endpoints**. Une liste des points terminaux API du service apparaît.
3. En fonction de la région géographique la plus proche de votre centre de données, notez l'URL du point terminal API du service de type **identité**.

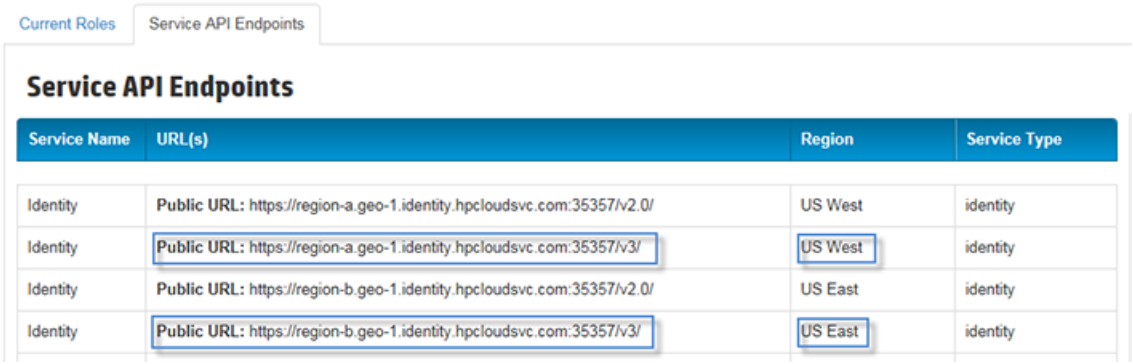
   Il sera indiqué ultérieurement dans le champ Service d'Authentification pendant la création du dispositif de Cloud (Helion) dans le GUI HPE Data Protector.

   Si vous décidez d'utiliser les touches d'accès pour l'authentification, notez l'adresse URL du service d'authentification se terminant par le suffixe **/v3/**.

   Par exemple :

   https://region-b.geo-1.identity.hpcloudsvc.com:35357**/v3/**

Service API Endpoints dans HPE Public Cloud

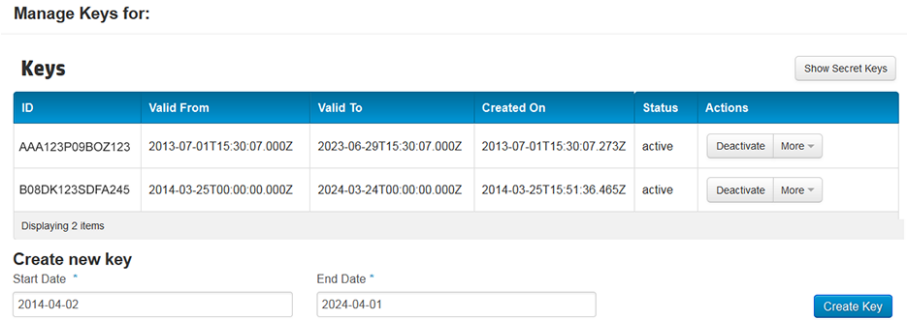


Création des clés d'accès

Procédure

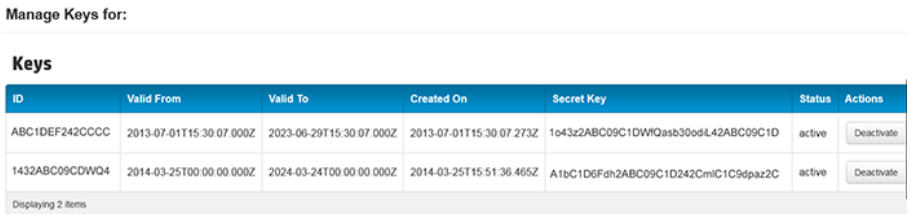
1. Dans le menu Utilisateur, sélectionnez **Manage Access Keys**. La page Manage Access Keys s'ouvre.
2. Pour créer une nouvelle clé, spécifiez une **date de début** et une **date de fin** pour la nouvelle clé, puis cliquez sur **Create Key**. La nouvelle clé est créée.

   Création des clés d'accès dans HPE Public Cloud



3. Cliquez sur **Show Secret Keys** pour afficher l'ID et les clés secrètes de la nouvelle clé.

   Clés Secrètes dans HPE Public Cloud



4. Copiez les informations concernant l'ID et les clés secrètes pour une utilisation ultérieure. Elles seront indiquées pendant la création du dispositif de Cloud (Helion) dans le GUI HPE Data Protector.

Configuration d'un périphérique de sauvegarde sur disque - Cloud (Helion)

Dans HPE Data Protector, configurez une sauvegarde vers le disque avec le dispositif de Cloud (Helion) de type interface.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
3. Indiquez le nom du périphérique et une description (facultatif).
4. Sélectionnez le type de dispositif **Sauvegarde vers Disque**, puis sélectionnez le type d'interface : **Cloud (Helion)**. Cliquez sur **Suivant**.
5. Spécifiez l'**URL du service d'authentification**. Il s'agit de l'URL du point terminal de l'API du service dans la rubrique Obtention de l'URL du service d'authentification.
6. Dans la liste **Mode d'authentificatio**n, sélectionnez un mode d'authentification.
   a. Pour utiliser l'authentification du nom d'utilisateur et mot de passe, sélectionnez **Nom d'utilisateur et mot de passe** et entrée vos codes d'accès HPE Public Cloud.
   b. Pour utiliser des clés d'accès pour l'authentification, sélectionnez **Clés d'accès** et saisissez l'**ID clé d'accès** et la **clé secrète**. Il s'agit des clés spécifiées dans la rubrique Création des clés d'accès.

   > **REMARQUE :**
   > Pour utiliser les touches d'accès pour l'authentification, l'URL du service d'authentification doit contenir le suffixe **/v3/**. Par exemple :
   >
   > https://region-b.geo-1.identity.hpcloudsvc.com:35357**/v3/**
7. Spécifiez le **Locataire / Projet**. Il s'agit du nom de projet spécifié dans la rubrique Obtention du nom du projet.
8. Cliquez sur **Sélectionner/créer un conteneur** pour sélectionner les conteneurs dans une liste de conteneurs existants ou pour créer un nouveau conteneur.
9. Spécifiez une passerelle locale vers la source de données.
   a. Sélectionnez une passerelle et cliquez sur **Ajouter** pour afficher la boîte de dialogue des propriétés. Si nécessaire, modifiez les propriétés de la passerelle puis cliquez sur **OK** pour l'ajouter.
10. Cliquez sur **Suivant** pour afficher la fenêtre Résumé. Vérifiez les paramètres et cliquez sur **Terminer**. Le dispositif récemment configuré s'affiche dans le volet d'exploration.

Configuration d'un périphérique de sauvegarde sur disque - Cloud (Azure)

Dans Data Protector, configurez un périphérique de sauvegarde sur disque à l'aide du **Type d'interface** Cloud (Azure).

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
3. Spécifiez un nom de périphérique dans le champ **Nom du périphérique**. Sa **Description** est facultative.
4. Sélectionnez le type de périphérique **Sauvegarde sur disque**, puis le **Type d'interface** : Cloud (Azure) Cliquez sur **Suivant**.

   L'**URL de la console de gestion** est saisie par défaut.
5. Saisissez le **Nom du compte de stockage**, la **Clé secrète** et la **Clé secrète 2** dans les champs correspondants. Cliquez sur **Ajouter** pour ajouter une passerelle pour envoyer les données vers Cloud (Azure). La fenêtre Sélectionner un conteneur s'affiche.
6. Sélectionnez un conteneur existant ou créez-en un nouveau pour télécharger les données. La passerelle peut être ajoutée avec les valeurs par défaut.

   Il existe une limite de taille de bloc pour la copie d'objets. Si vous effectuez la copie d'objets d'un périphérique local vers le cloud, puis à nouveau sur le même périphérique pour restauration, la taille de bloc du périphérique local et celle du périphérique cloud doivent correspondre.
7. Cliquez sur **Vérifier** pour vérifier que la passerelle est connectée à Cloud (Azure). Si la connexion réussit, l'état affiché est **OK**. Le périphérique est créé et est prêt à l'emploi.

Configuration d'un périphérique de bibliothèque de fichiers

Notez que le disque sur lequel réside le périphérique de bibliothèque de fichiers doit être local pour l'Agent de support. Sinon, les performances du périphérique risquent d'être diminuées.

Conditions préalables

- Le disque sur lequel le périphérique de bibliothèque de fichiers résidera doit être visible dans le système de fichiers dans lequel réside le périphérique de bibliothèque de fichiers.
- Le répertoire dans lequel le contenu du périphérique de bibliothèque de fichiers doit être créé doit exister sur le disque où le périphérique de bibliothèque de fichiers résidera.
- Si vous créez un périphérique de bibliothèque de fichiers sur un système Windows, désactivez l'option de compression Windows pour un fichier que vous souhaitez utiliser comme périphérique de bibliothèque de fichiers.

Limites

- Le périphérique de bibliothèque de fichiers peut inclure un ou plusieurs répertoires. Un seul répertoire peut se trouver dans un système de fichiers.
- La longueur des chemins d'accès vers les répertoires qui peuvent être utilisés pour configurer les périphériques de type bibliothèque de fichiers ne peut pas dépasser 46 caractères.

Procédure

1. Créez un répertoire pour le dispositif de librairie de fichiers sur le disque sur lequel vous souhaitez placer le dispositif, par exemple : `c:\FileLibrary`.

   Un périphérique de bibliothèque de fichiers peut être créé sur un disque local ou réseau (ou un système de fichiers NFS monté sur des systèmes UNIX). Le disque de réseau peut être indiqué dans le formulaire `\\hostname\share_name` ou peut être mappé vers une lettre de disque (`S:\datastore\My_FileLibrary`).

   Les noms d'hôtes et leurs noms de partages ainsi que les lecteurs réseau n'apparaissent pas dans la boîte de dialogue Explorer lecteurs où vous saisissez le chemin. Vous devez vous-même entrer le chemin des noms UNC ou des lecteurs réseau.

   Sur un système d'exploitation **Windows**, pour obtenir les bonnes autorisations pour accéder au disque partagé sur lequel un dispositif de bibliothèque de fichiers se trouve, modifiez le compte Inet Data Protector sur l'Agent de Support (en lui donnant l'autorisation d'accéder au système client local et aux disques partagés à distance). En outre, assurez-vous qu'il s'agit d'un compte utilisateur spécifique, et non du compte système. Après avoir configuré le compte Inet, vous pouvez configurer et utiliser les périphériques de bibliothèque de fichiers sur des disques partagés.

   > **IMPORTANT :**
   > Il est essentiel que le répertoire créé pour la bibliothèque de fichiers ne soit supprimé du disque. S'il est supprimé, toutes les données sur le périphérique de bibliothèque de fichiers seront perdues.

2. Dans la liste contextuelle du Gestionnaire Data Protector, cliquez sur **Périphériques et supports**.
3. Dans le volet d'exploration, cliquez droit sur **Dispositifs** puis cliquez sur **Ajouter Dispositifs** pour ouvrir l'assistant.
4. Dans la zone de texte Nom du périphérique, entrez un nom pour le périphérique de bibliothèque de fichiers.
5. Dans la zone de texte Description, vous pouvez saisir une description de la bibliothèque (facultatif).
6. Dans la liste Type de périphérique, sélectionnez **Bibliothèque de fichiers**.
7. Dans la liste déroulante Client, sélectionnez le système client sur lequel résidera le périphérique. Cliquez sur **Suivant**.
8. Spécifiez un répertoire ou un groupe de répertoires dans lequel vous voulez stocker la bibliothèque de fichiers. Cliquez sur **Ajouter**.
9. Pour afficher les propriétés par défaut d'un répertoire, sélectionnez le répertoire puis cliquez sur **Propriétés**.
10. Entrez le nombre de modules d'écriture sur la bibliothèque de fichiers. Il s'agit par défaut du nombre de répertoires que vous avez ajoutés. Si vous ajoutez plus de modules d'écriture que le nombre de répertoires dans le périphérique, vous pouvez peut-être améliorer les performances du périphérique. Cela dépend de votre configuration matérielle. Vous aurez besoin de tester cette configuration dans votre environnement. Cliquez sur **Suivant**.
11. Le type de support du périphérique de bibliothèque de fichiers est Fichier. Pour activer la sauvegarde complète virtuelle au sein de cette bibliothèque de fichiers, sélectionnez **Utiliser le**

format de support de fichiers distribués. Cliquez sur **Suivant**.

12. Consultez le résumé de la configuration du périphérique de bibliothèque de fichiers. Cliquez sur **Terminer** pour quitter l'assistant.

Le nom du périphérique s'affiche dans la liste de périphériques configurés. Le nom du périphérique apparaît également dans le pool de supports auquel le périphérique a été affecté.

Les dépôts de fichiers n'apparaîtront pas dans le périphérique jusqu'à ce qu'il soit utilisé pour la première fois.

Vous pouvez analyser le périphérique pour vérifier la configuration après que le périphérique a été utilisé pour la première fois.

Par défaut, la stratégie d'utilisation des supports du pool de supports utilisée par la bibliothèque de fichiers est Sans possibilité d'ajout. L'utilisation de cette stratégie est recommandée car elle vous offre les avantages de la bibliothèque de fichiers, notamment la réutilisation automatique des supports expirés. En outre, pour effectuer une copie ou une consolidation d'objets en utilisant la bibliothèque de fichiers, la stratégie d'utilisation des supports Sans possibilité d'ajout est nécessaire.

Configuration de plusieurs chemins d'accès aux périphériques

Un périphérique installé dans un environnement SAN est généralement connecté à plusieurs clients ; il est donc accessible par plusieurs chemins d'accès, c'est-à-dire au moyen de différents noms et adresses SCSI de clients (fichiers de périphérique sur les systèmes UNIX). Data Protector peut utiliser n'importe lequel de ces chemins. Vous pouvez configurer tous les chemins d'accès à un périphérique physique sous la forme d'un périphérique logique unique (*périphérique MultiPath*).

Par exemple, un dispositif de bande est connecté à client1 et configuré comme `/dev/rs1` et `/dev/rs2`, sur client2 comme `/dev/r1s1` et sur client3 comme `scsi1:0:1:1`. Vous pouvez alors y accéder par quatre chemins : `client1:/dev/rs1`, `client1:/dev/rs2`, `client2:/dev/r1s1` et `client3:scsi1:0:1:1`. Un périphérique MultiPath contient donc les quatre chemins d'accès à ce périphérique à bandes.

Utilité des chemins multiples

Les versions antérieures de Data Protector permettaient d'accéder à chaque périphérique à partir d'un seul client. Pour pallier ce problème, il fallait configurer plusieurs périphériques logiques pour un périphérique physique via un nom de verrouillage. Ainsi, si vous utilisiez des noms de verrouillage pour configurer l'accès à un périphérique physique unique depuis différents systèmes, vous deviez configurer tous les périphériques sur chacun des systèmes. Par exemple, pour 10 clients connectés à un seul périphérique, vous deviez configurer 10 périphériques avec le même nom de verrouillage. Cette version de Data Protector permet de simplifier la configuration en configurant un seul périphérique multichemins pour l'ensemble des chemins.

Les périphériques MultiPath augmentent la résilience des systèmes. Data Protector tentera d'utiliser le premier chemin défini. Si tous les chemins sur un client sont inaccessibles, Data Protector essaiera d'utiliser les chemins sur le client suivant. La session est abandonnée si tous les chemins répertoriés sont indisponibles.

Sélection des chemins

Lors d'une session de sauvegarde, les chemins du périphérique sont sélectionnés dans l'ordre défini durant la configuration de ce périphérique, sauf si un client recommandé est défini dans la spécification de sauvegarde. Dans ce cas, c'est ce client qui est utilisé en premier.

Lors d'une session de restauration, les chemins sont sélectionnés dans l'ordre suivant :

1. Chemins qui se trouvent sur le client sur lequel les objets sont restaurés, si *tous* les objets sont restaurés sur le même client cible
2. Chemins utilisés pour la sauvegarde
3. Autres chemins disponibles

Pour les périphériques comportant plusieurs chemins configurés, les chemins locaux sont utilisés en premier. Si aucun chemin local n'est disponible, tout chemin existant dans l'ordre prédéfini est utilisé.

Si l'accès direct à la bibliothèque est activé, ce sont les chemins locaux (sur le client cible) qui sont utilisés en premier, quel que soit l'ordre défini.

Le Backup Session Manager (BSM) Data Protector utilise des périphériques locaux autant que possible dans les environnements SAN MultiPath. Vous pouvez ajuster ce comportement à l'aide de `LANfree` l'option globale.

L'option globale `LANfree` a deux valeurs possibles :

- 0 – est la valeur par défaut. Aucun changement n'est nécessaire pour les versions antérieures HPE Data Protector à 8.11.
- 1 – s'applique à un environnement MultiPath dans lequel HPE Data Protector sélectionne l'hôte d'où vient l'objet (si ce chemin est disponible) au lieu de sélectionner l'hôte préféré ou le premier hôte dans la liste MultiPath.

  Ce qui suit décrit les améliorations d'attribution de dispositif à chemins multiples réelles lorsque l'option globale LANfree est définie comme 1 :

  - HPE Data Protector préfère l'host d'où les données proviennent pour un dispositif qui a configuré le chamin d'accès vers cet host.
  - HPE Data Protector préfère un nouvel Agent de support (MA) sur l'hôte d'où proviennent les données pour un périphérique dont le chemin est configuré vers cet hôte. Cela est fait si un AS à distance a déjà été démarré pour le dispositif cible avec un créneau coïncidant libre

HPE Data Protector risque néanmoins de ne pas utiliser les chemins locaux pour les périphériques dans les scénarios suivants :

- Si un utilisateur a spécifié un partage de charge (paramètres MIN ou MAX), le BSM peut choisir et verrouiller les périphériques qui ne sont pas locaux pour tous les hôtes d'où proviennent les données.
- Si un MA contrôlant un périphérique MultiPath s'exécute sur un hôte, et qu'un objet provient d'un autre hôte dont le chemin pointe vers ce périphérique, Data Protector ne migrera pas le MA vers l'hôte local mais enverra via le LAN les données au MA déjà démarré. Cela se produit lorsque la valeur MAX de partage de charge a déjà été atteinte.
- Le paramètre `LANfree` est désactivé lorsque l'option globale `IgnoreObjectLocalityForDeviceSelection` est définie. Par défaut, le `IgnoreObjectLocalityForDeviceSelection` n'est pas défini.

Dans les cas suivants, l'utilisateur devra éventuellement ajouter des chemins de périphériques supplémentaires pour effectuer des sauvegardes sans LAN :

- Quand un client de sauvegarde comporte plusieurs interfaces réseau et noms d'hôte. Dans ce cas, selon la configuration DNS, les sauvegardes HPE Data Protector peuvent transiter par plusieurs interfaces. L'ajout de chemins locaux pour chaque interface serait alors recommandé.
- Lorsque vous effectuez une sauvegarde de système de fichiers d'un serveur de fichiers Windows représentant une ressource cluster Windows. Dans une telle configuration, chaque ressource cluster Windows a son propre nom d'hôte pour lequel il faut créer une entrée de chemin de périphérique distincte.

Compatibilité avec les versions antérieures

Les périphériques configurés avec les versions précédentes de Data Protector ne sont pas reconfigurés pendant une mise à niveau ; ils peuvent être utilisés comme dans les versions précédentes de Data Protector, sans aucune modification. Pour exploiter la nouvelle fonctionnalité de chemins multiples, reconfigurez les périphériques en tant que périphériques MultiPath.

Limites

Les limites applicables sont les suivantes :

- Les chemins multiples ne sont pas pris en charge pour les périphériques NDMP et les bibliothèques de bandes magnéto-optiques.
- Les chaînes de périphériques ne sont pas prises en charge pour les périphériques MultiPath.

Définition des options avancées des périphériques et des supports

Vous pouvez définir des options avancées pour les périphériques et les supports lors de la configuration d'un nouveau périphérique ou lors de la modification des propriétés d'un périphérique. La disponibilité de ces options dépend du type de périphérique utilisé.

Certaines de ces options peuvent aussi être définies lors de la configuration d'une sauvegarde. Les options de périphérique définies dans une spécification de sauvegarde prévalent sur celles qui le sont pour le périphérique en général.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Périphériques**.
3. Cliquez avec le bouton droit sur le périphérique (le lecteur dans le cas de périphériques de bibliothèque) dont vous souhaitez modifier les options, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Paramètres**, puis sur le bouton **Avancé** pour ouvrir les pages Options avancées : **Paramètres**, **Tailles** et **Autres**.
5. Indiquez les options de votre choix et cliquez sur **OK** pour appliquer les modifications.

Configuration d'un périphérique VTL

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Environnement**, cliquez avec le bouton droit de la souris sur **Périphériques** puis sélectionnez **Ajouter périphérique** pour ouvrir l'assistant.
3. Dans la zone de texte Nom de périphérique, saisissez le nom de la VTL.
4. Dans la zone de texte Description, vous pouvez saisir une description (facultatif).
5. Vous pouvez également sélectionner **Périphérique MultiPath**.
6. Dans la liste Type de périphérique, sélectionnez **Bibliothèque SCSI**. **SCSI** est alors sélectionné automatiquement dans la liste Type d'interface.
7. Si l'option **Périphérique MultiPath** n'est *pas* sélectionnée, sélectionnez le nom du client dans la liste de clients.
8. Dans la zone de texte relative à l'adresse **URL de la console de gestion**, entrez une URL valide pour la console de gestion de bibliothèque (facultatif). Cliquez sur **Suivant**.
9. Spécifiez les informations requises sur l'adresse la de bibliothèque SCSI et la gestion du lecteur, puis cliquez sur **Suivant**.
10. Spécifiez les emplacements à utiliser avec Data Protector, puis cliquez sur **Suivant**.
11. Sélectionnez le type de support qui sera utilisé avec le périphérique.
12. Cliquez sur **Terminer** pour quitter l'assistant.

> **REMARQUE :** Si vous utilisez le périphérique VTL sur des systèmes RedHat Linux (RHEL) 7.1, vous devez charger manuellement le lecteur générique SCSI. Pour cela, exécutez la commande `modprobe -vs sg`. Nous vous recommandons aussi d'ajouter cette commande au RHEL `init scripts` ou `cron job` pour assurer que cette commande est lancée dès que le système démarre.

Configuration d'un périphérique chargeur

Une fois que le périphérique de sauvegarde est connecté au système et qu'un fichier de périphérique de travail (adresse SCSI) existe, vous pouvez configurer le périphérique pour pouvoir l'utiliser avec Data Protector.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
3. Dans la zone de texte Nom de périphérique, saisissez le nom du périphérique.
4. Dans la zone de texte Description, vous pouvez saisir une description (facultatif).
5. Vous pouvez également sélectionner **Périphérique MultiPath**.

6. Si l'option **Périphérique MultiPath** n'est pas sélectionnée, sélectionnez le nom du client.
7. Cliquez sur **Suivant**.
8. Dans la liste Type de périphérique, sélectionnez le type de périphérique **Chargeur**, puis cliquez sur **Suivant**.
9. Dans la zone de texte Périphérique de données, saisissez l'adresse SCSI du périphérique physique (systèmes Windows) ou le nom de fichier de périphérique (systèmes UNIX). Vous pouvez aussi utiliser la flèche de défilement vers le bas pour détecter automatiquement les adresses ou les noms de fichier de lecteurs.

   Pour les périphériques MultiPath, sélectionnez également le nom du client et cliquez sur **Ajouter** pour ajouter le chemin d'accès à la liste des chemins configurés.
10. Sélectionnez l'option **Découvrir automatiquement adresse SCSI modifiée** pour activer la détection automatique des adresses SCSI modifiées.
11. Cliquez sur **Suivant**.
12. Dans la liste déroulante Type de support, sélectionnez un type de support pour le périphérique que vous êtes en train de configurer.
13. Indiquez un pool de supports pour le type de support sélectionné. Vous pouvez soit sélectionner un pool dans la liste déroulante Pool de supports, soit saisir un nouveau nom de pool. Dans ce cas, le pool sera créé automatiquement.
14. Cliquez sur **Terminer** pour quitter l'assistant.

Le nom du périphérique s'affiche dans la liste de périphériques configurés. Vous pouvez analyser le périphérique pour en vérifier la configuration. Si le périphérique est correctement configuré, Data Protector peut charger, lire et décharger des supports dans les emplacements.

Gestion des supports d'un périphérique chargeur

Une fois un périphérique chargeur configuré, notez que la gestion de ses supports présente certaines particularités. Par exemple, il faut effectuer séparément les opérations d'analyse, de vérification ou de formatage sur chacun de ses supports. Vous devez charger correctement un support pour pouvoir exécuter des sessions Data Protector.

Configuration d'un périphérique de bibliothèque de bandes magnéto-optiques

Une fois que le périphérique de sauvegarde est connecté au système et qu'un fichier de périphérique de travail (adresse SCSI) existe, vous pouvez configurer le périphérique pour pouvoir l'utiliser avec Data Protector.

Configuration d'un périphérique de bibliothèque de bandes magnéto-optiques

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
3. Dans la zone de texte Nom de périphérique, saisissez le nom du périphérique.
4. Dans la zone de texte Description, vous pouvez saisir une description (facultatif).
5. Dans la liste Type de périphérique, sélectionnez **Bibliothèque de bandes magnéto-optiques**.
6. Dans la liste Client, sélectionnez le nom du client.
7. Dans la zone de texte relative à l'adresse **URL de la console de gestion**, entrez une URL valide pour la console de gestion de bibliothèque (facultatif).
8. Cliquez sur **Suivant**.
9. Indiquez un ensemble de fichiers/disques pour la bibliothèque de bandes magnéto-optiques. Utilisez un tiret pour spécifier plusieurs fichiers ou disques à la fois (`/tmp/FILE 1-3`, par exemple), puis cliquez sur **Ajouter**. Pour les bibliothèques de bandes magnéto-optiques, les noms de disque doivent se terminer par `A/a` ou `B/b`. Cliquez sur **Suivant**.
10. Dans la liste Type de support, sélectionnez un type de support pour le périphérique que vous êtes en train de configurer.
11. Cliquez sur **Terminer** pour quitter cet assistant. Il vous est alors demandé de configurer un lecteur de bibliothèque. Cliquez sur **Oui** pour afficher l'assistant de configuration.

Configuration d'un lecteur dans le périphérique de bibliothèque de stockage

Procédure

1. Dans la zone de texte Nom de périphérique, saisissez le nom du périphérique.
2. Dans la zone de texte Description, vous pouvez éventuellement saisir une description.
3. Indiquez un pool de supports pour le type de support sélectionné. Vous pouvez soit sélectionner un pool dans la liste Pool de supports, soit saisir un nouveau nom de pool. Dans ce cas, le pool sera créé automatiquement. Vous pouvez configurer un pool de supports pour tous les lecteurs ou choisir un pool de supports indépendant pour chaque lecteur. Cliquez sur **Suivant**.
4. Le cas échéant, vous pouvez aussi sélectionner **Le périphérique peut être utilisé pour la restauration** et/ou **Le périphérique peut être utilisé comme source pour la copie d'objets** et indiquer une **balise de périphérique**.
5. Cliquez sur **Terminer** pour quitter l'assistant.

Le nom du lecteur s'affiche dans la liste des lecteurs configurés. Vous pouvez analyser les lecteurs pour en vérifier la configuration.

Configuration d'une bibliothèque SCSI ou d'un périphérique de magasin

Une fois que le périphérique de sauvegarde est connecté au système et qu'un fichier de périphérique de travail (adresse SCSI) existe, vous pouvez configurer le périphérique pour pouvoir l'utiliser avec Data Protector.

La procédure de configuration pour une bibliothèque et un support de magasin est la même, sauf que vous devez indiquer un pool de supports avec le jeu d'options **Support de magasin** lors de la configuration d'un périphérique magasin.

Il est recommandé de laisser Data Protector configurer automatiquement les périphériques de sauvegarde.

Configuration d'un robot de bibliothèque SCSI

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
3. Dans la zone de texte Nom de périphérique, saisissez le nom du périphérique.
4. Dans la zone de texte Description, vous pouvez saisir une description (facultatif).
5. Vous pouvez également sélectionner **Périphérique MultiPath**.
6. Dans la liste Type de périphérique, sélectionnez le type de périphérique **Bibliothèque SCSI**.
7. Dans la liste Type d'interface, sélectionnez le type d'interface **SCSI**.
8. Si l'option **Périphérique MultiPath** n'est *pas* sélectionnée, sélectionnez le nom du client dans la liste de clients.
9. Dans la zone de texte relative à l'adresse **URL de la console de gestion**, entrez une URL valide pour la console de gestion de bibliothèque (facultatif).
10. Cliquez sur **Suivant**.
11. Saisissez l'adresse SCSI du robot de bibliothèque ou utilisez la flèche de défilement vers le bas pour détecter automatiquement les adresses ou les noms de fichiers des lecteurs.

    Pour les périphériques MultiPath, sélectionnez également le nom du client et cliquez sur **Ajouter** pour ajouter le chemin d'accès à la liste des chemins configurés.
12. Dans la liste **Comportement en cas de lecteur occupé**, sélectionnez l'action que Data Protector doit effectuer si le lecteur est occupé.
13. Sélectionnez l'option **Découvrir automatiquement adresse SCSI modifiée** pour activer la détection automatique des adresses SCSI modifiées.
14. Sélectionnez optionnellement **Réservation/Libération SCSI (contrôle du robot)**. Cliquez sur **Suivant**.
15. Indiquez les emplacements du périphérique. Utilisez un tiret pour saisir des plages d'emplacements, puis cliquez sur **Ajouter**. Par exemple, saisissez 1-3 et cliquez sur **Ajouter** pour

ajouter les emplacements 1, 2 et 3 en même temps. N'utilisez pas de lettres ou de zéros non significatifs. Cliquez sur **Suivant**.

16. Dans la liste déroulante Type de support, sélectionnez un type de support pour le périphérique que vous êtes en train de configurer.
17. Cliquez sur **Terminer** pour quitter cet assistant. Il vous est alors demandé de configurer un lecteur de bibliothèque. Cliquez sur **Oui** pour faire apparaître l'assistant de configuration du lecteur.

Configuration d'un lecteur dans une bibliothèque

Procédure

1. Dans la zone de texte Nom de périphérique, saisissez le nom du périphérique.
2. Dans la zone de texte Description, vous pouvez éventuellement saisir une description.
3. Vous pouvez également sélectionner **Périphérique MultiPath**.
4. Si l'option **Périphérique MultiPath** n'est *pas* sélectionnée, sélectionnez le nom du client dans la liste de clients.

   > **CONSEIL :**
   > Vous pouvez configurer une bibliothèque de manière à ce que chaque lecteur puisse recevoir des données provenant d'un système différent disposant d'un Agent de support Data Protector. Cela permet d'obtenir de meilleures performances dans les environnements haute résolution. Dans la liste déroulante Client, sélectionnez le système client que vous voulez utiliser pour chaque lecteur.

   Cliquez sur **Suivant**.
5. Dans la zone de texte Lecteur de données, saisissez l'adresse SCSI du lecteur de données ou son nom de fichier.

   Pour les périphériques MultiPath, sélectionnez également le nom du client et cliquez sur **Ajouter** pour ajouter le chemin d'accès à la liste des chemins configurés.
6. Sélectionnez l'option **Découvrir automatiquement adresse SCSI modifiée** pour activer la détection automatique des adresses SCSI modifiées.
7. Dans la zone de texte Index de lecteur, saisissez l'index du lecteur dans la bibliothèque. Cliquez sur **Suivant**.
8. Indiquez un pool de supports pour le type de support sélectionné. Vous pouvez soit sélectionner un pool dans la liste déroulante Pool de supports, soit saisir un nouveau nom de pool. Dans ce cas, le pool sera créé automatiquement. Il est recommandé d'utiliser le pool de supports par défaut.

   > **REMARQUE :**
   > Il n'est pas nécessaire de configurer tous les lecteurs à utiliser avec Data Protector. Vous pouvez configurer un pool de supports pour tous les lecteurs ou choisir un pool de supports indépendant pour chaque lecteur.

   Lors de la spécification du pool de supports pour un périphérique magasin, sélectionnez-en un avec le jeu d'options **Support de magasin**.

   Cliquez sur **Suivant**.

9. Le cas échéant, vous pouvez aussi sélectionner **Le périphérique peut être utilisé pour la restauration** et/ou **Le périphérique peut être utilisé comme source pour la copie d'objets** et indiquer une **balise de périphérique**.
10. Cliquez sur **Terminer** pour quitter l'assistant.

Le nom du lecteur s'affiche dans la liste des lecteurs configurés. Vous pouvez analyser les lecteurs pour en vérifier la configuration. Si le périphérique est correctement configuré, Data Protector peut charger, lire et décharger des supports dans les emplacements.

Configuration de périphériques dans un environnement SAN

L'environnement SAN peut varier d'un client utilisant une bibliothèque à plusieurs clients utilisant plusieurs bibliothèques. Les clients peuvent avoir différents systèmes d'exploitation. Du point de vue de Data Protector, la configuration d'un environnement SAN vise les objectifs suivants :

- Sur chaque hôte qui partagera le robot de la bibliothèque, créez une définition du robot de la bibliothèque pour chaque hôte. Si un seul hôte contrôle le robot, la définition de la bibliothèque est créée uniquement pour l'hôte de contrôle du robot par défaut.
- Sur chaque hôte qui participera au partage des mêmes lecteurs (bandes) de la bibliothèque :
  - Créez une définition de périphérique pour chaque périphérique à utiliser.
  - Utilisez un nom de verrouillage si le périphérique (physique) sera également utilisé par un autre hôte (périphérique partagé).
  - Vous pouvez également sélectionner un accès direct si vous souhaitez utiliser cette fonctionnalité. Si vous l'utilisez, vérifiez que le fichier `libtab` est configuré sur cet hôte.

Points à prendre en considération

- Microsoft Cluster Server : Assurez-vous que le chemin matériel du lecteur est le même sur les deux noeuds du cluster : une fois le périphérique configuré, effectuez un basculement afin de le vérifier.

Méthodes de configuration

Il existe trois méthodes de configuration qui dépendent des plates-formes participant à la configuration SAN :

Configuration automatique des périphériques en utilisant l'interface graphique

Vous pouvez utiliser la fonctionnalité de configuration automatique de Data Protector pour configurer automatiquement les périphériques et les bibliothèques sur plusieurs hôtes dans un environnement SAN. La configuration automatique est possible sur les systèmes d'exploitation suivants :

- Windows
- HP-UX

- Solaris
- Linux
- AIX

Limites

La configuration automatique ne peut pas être utilisée pour configurer les périphériques suivants dans un environnement SAN :

- bibliothèques de supports mixtes,
- bibliothèques DAS ou ACSLS,
- périphériques NDMP.

Data Protector découvre les périphériques de sauvegarde connectés à votre environnement. Pour les périphériques de bibliothèque, Data Protector détermine le nombre d'emplacements, le type de support et les lecteurs qui appartiennent à la bibliothèque. Data Protector configure ensuite le périphérique en définissant un nom logique, un nom de verrouillage, le type de support et l'adresse du fichier ou l'adresse SCSI du périphérique, ainsi que le lecteur et les emplacements.

> **REMARQUE :**
> Lorsque vous ajoutez un hôte dans un environnement SAN, les bibliothèques et les périphériques configurés ne sont pas mis à jour automatiquement.
>
> - Pour utiliser une bibliothèque existante sur un nouvel hôte, supprimez celle-ci et configurez-en automatiquement une nouvelle avec le même nom sur le nouvel hôte.
> - Pour ajouter des périphériques à une bibliothèque existante, vous pouvez supprimer la bibliothèque puis en configurer automatiquement une nouvelle avec le même nom et les nouveaux lecteurs sur un nouvel hôte ou ajouter manuellement les lecteurs à la bibliothèque.

Configuration automatique des périphériques en utilisant l'interface de ligne de commande (commande sanconf)

Vous pouvez configurer les périphériques et les bibliothèques d'un environnement SAN à l'aide de la commande `sanconf`. La commande `sanconf` est un utilitaire qui facilite la configuration des bibliothèques d'environnements SAN dans des cellules Data Protector uniques ainsi que dans des environnements MoM avec une base de données centralisée de gestion des supports (Centralized Media Management Database ou CMMDB). Elle peut configurer automatiquement une bibliothèque d'un environnement SAN en recueillant des informations sur les lecteurs de plusieurs clients puis en configurant ces clients dans une seule bibliothèque. Dans des environnements MoM, `sanconf` permet également de configurer toute bibliothèque d'une cellule Data Protector qui utilise CMMDB, à condition que la cellule dans laquelle `sanconf` est exécutée exécute également CMMDB. `sanconf` est disponible sur les systèmes d'exploitation suivants :

- Windows
- HP-UX
- Solaris

`sanconf` peut détecter et configurer les périphériques pris en charge et connectés à des clients exécutés sur les systèmes d'exploitation suivants :

- Windows
- HP-UX
- Solaris
- Linux
- AIX

Avec cette commande, vous pouvez :

- Analyser le système Data Protector spécifié afin de recueillir des informations sur les adresses SCSI des lecteurs et des contrôles de robots connectés aux clients dans l'environnement SAN.
- Configurer ou modifier les paramètres d'une bibliothèque ou d'un lecteyr pour des clients donnés en utilisant les informations recueillies lors de l'analyse des clients Data Protector.
- Supprimer les lecteurs de tous les clients ou de clients spécifiés d'une bibliothèque.

Verrouillage de périphérique

La commande `sanconf` crée automatiquement des noms de verrouillage pour les lecteurs qu'elle configure. Un nom verrouillage se compose de la chaîne ID fournisseur, de la chaîne ID produit et du numéro de série du produit.

Par exemple, le nom de verrouillage du lecteur HPE DLT 8000 avec l'ID fournisseur "HP", l'ID produit "DLT8000" et le numéro de série "A1B2C3D4E5" sera HP:DLT8000:A1B2C3D4E5.

Les noms de verrouillage peuvent également être ajoutés manuellement. Les noms de verrouillage sont uniques à chaque périphérique logique.

Vous ne devez pas modifier les noms de verrouillage qui ont été créés par la commande `sanconf`. Tous les autres lecteurs logiques créés manuellement et qui représentent des lecteurs physiques configurés par `sanconf` doivent également utiliser des noms de verrouillage créés par `sanconf`.

Limites

- Pour obtenir une liste complète des bibliothèques prises en charge par la commande `sanconf`, consultez les dernières matrices de support à l'adresse .https://softwaresupport.hpe.com/
- `sanconf` n'offre pas les fonctionnalités suivantes :
  - Installation de lecteurs de rechange dans les emplacements des lecteurs.
  - Combinaison de différents types de lecteurs ; par exemple, des combinaisons de lecteurs DLT, 9840 et LTO.
  - Configuration de clients actuellement indisponibles. La configuration de tels clients n'est possible que si la configuration de la bibliothèque est effectuée à l'aide d'un fichier de configuration contenant les informations recueillies après analyse des clients.

Recommandation

Configurez un seul pilote pour un périphérique spécifique sur un système.

Pour plus d'informations sur l'utilisation de la commande `sanconf`, reportez-vous à la page de manuel `sanconf` ou à la *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Configuration manuelle sur des systèmes UNIX

Lorsque vous configurez manuellement des périphériques partagés connectés aux systèmes UNIX d'un environnement SAN, vous devez:

- Créez une définition de périphérique pour chaque périphérique à utiliser.
- Utiliser un nom de verrouillage.
- Vous pouvez également sélectionner un accès direct si vous souhaitez utiliser cette fonctionnalité. Dans ce cas, vous devez vérifier que le fichier `libtab`sur cet hôte est correctement configuré.

Phases

1. Configurer manuellement les périphériques
2. Configurer manuellement le fichier libtab

Configuration manuelle de périphériques dans un environnement SAN

La procédure suivante suppose que le lecteur et le robot sont utilisés par plusieurs systèmes, que le disque est utilisé par plusieurs applications (pas seulement Data Protector), et que tous les systèmes envoient des commandes de contrôle du robot (accès direct à la bibliothèque). Les tâches suivantes fournissent également d'autres possibilités d'utilisation si votre environnement est différent.

Pour le contrôle du robot, vous pouvez utiliser n'importe quel client dans l'environnement SAN. Vous devez d'abord configurer le contrôle du robot de la bibliothèque sur un client qui agit comme le système de contrôle du robot par défaut. Ce client servira à gérer les déplacements de supports, quel que soit le client qui demande le déplacement de supports. Cela permet d'éviter les conflits au niveau des robots si plusieurs hôtes demandent en même temps le déplacement de supports. Seul en cas de défaillance de l'hôte et si l'accès direct est activé, le contrôle du robot est effectué par l'hôte local qui demande le déplacement des supports.

Conditions préalables

Un Agent de support Data Protector (Agent de support général ou Agent de support NDMP) doit être installé sur chaque client qui a besoin de communiquer avec la bibliothèque partagée.

Etapes de la configuration

Configuration d'une bibliothèque dans un environnement SAN

Configuration d'un lecteur dans une bibliothèque

Configuration d'une bibliothèque dans un environnement SAN

> **REMARQUE :**
> Si vous voulez que le contrôle du robot soit géré par un cluster, vous devez vous assurer que :

- Le contrôle du robot existe sur chaque nœud de cluster.
- Le nom du cluster virtuel est utilisé dans la configuration du robot de la bibliothèque.
- La rorbotique et les noms de fichiers de dispositif courants sont installés soit à l'aide de la commande `mksf` soit à l'aide du fichier `libtab`.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
3. Dans la zone de texte Nom de périphérique, saisissez le nom du périphérique.
4. Dans la zone de texte Description, saisissez une description.
5. Vous pouvez également sélectionner **Périphérique MultiPath**.
6. Dans la liste déroulante Type de périphérique, sélectionnez le type de périphérique **Bibliothèque SCSI**.
7. Dans la liste déroulante Type d'interface, sélectionnez le type d'interface **SCSI**.
8. Si l'option **Périphérique MultiPath** n'est pas sélectionnée, sélectionnez le nom du client dans la liste déroulante Client.
9. Dans la zone de texte relative à l'adresse **URL de la console de gestion**, entrez une URL valide pour la console de gestion de bibliothèque (facultatif).
10. Cliquez sur **Suivant**.
11. Saisissez l'adresse SCSI du robot de bibliothèque ou utilisez la flèche de défilement vers le bas pour détecter automatiquement les adresses ou les noms de fichiers des lecteurs.

    Pour les périphériques MultiPath, sélectionnez également le nom du client dans la liste déroulante Client. Cliquez sur **Ajouter** pour ajouter le chemin d'accès à la liste des chemins configurés.
12. Dans la liste **Comportement en cas de lecteur occupé**, sélectionnez **Ejecter support**.
13. Sélectionnez **Découvrir automatiquement adresse SCSI modifiée** si vous souhaitez activer la découverte automatique d'adresses SCSI modifiées. Cliquez sur **Suivant**.
14. Indiquez les emplacements du périphérique. Utilisez un tiret pour saisir plusieurs emplacements à la fois, puis cliquez sur **Ajouter**. Par exemple, saisissez 1-3 et cliquez sur **Ajouter** pour ajouter les emplacements 1, 2 et 3 en même temps. Cliquez sur **Suivant**.
15. Dans la liste déroulante Type de support, sélectionnez un type de support pour le périphérique que vous êtes en train de configurer.
16. Cliquez sur **Terminer** pour quitter cet assistant. Il vous est alors demandé de configurer un lecteur de bibliothèque. Cliquez sur **Oui** pour faire apparaître l'assistant de configuration du lecteur. Suivez l'assistant comme décrit dans la tâche ci-dessous.

Configuration d'un lecteur dans une bibliothèque

Configurez chaque lecteur sur chaque client à partir duquel vous voulez l'utiliser.

Procédure

1. Dans la zone de texte Nom de périphérique, saisissez le nom du lecteur.

   Il est recommandé d'utiliser l'appellation suivante :

   - `LibraryLogicalName_DriveIndex_Hostname`, par exemple SAN_LIB_2_hotdog (pour les dispositifs sans chemins d'accès multiples)
   - `LibraryLogicalName_DriveIndex`, par exemple SAN_LIB_2 (pour les dispositifs aux chemins d'accès multiples)

2. Dans la zone de texte Description, saisissez une description.
3. Vous pouvez aussi sélectionner **Périphérique MultiPath**.
4. Si l'option **Périphérique MultiPath** n'est pas sélectionnée, sélectionnez le nom du client dans la liste déroulante Client.
5. Cliquez sur **Suivant**.
6. Dans la zone de texte Lecteur de données, saisissez l'adresse SCSI du lecteur de données ou son nom de fichier.

   Pour les périphériques MultiPath, sélectionnez également le nom du client dans la liste déroulante Client. Cliquez sur **Ajouter** pour ajouter le chemin d'accès à la liste des chemins configurés.
7. Dans la zone de texte Index de lecteur, saisissez l'index du lecteur dans la bibliothèque.
8. Sélectionnez **Découvrir automatiquement adresse SCSI modifiée** si vous souhaitez activer la découverte automatique d'adresses SCSI modifiées. Cliquez sur **Suivant**.
9. Indiquez un pool de supports pour le type de support sélectionné. Vous pouvez soit sélectionner un pool dans la liste déroulante Pool de supports, soit saisir un nouveau nom de pool. Dans ce cas, le pool sera créé automatiquement.

   Vous pouvez configurer un pool de supports pour tous les lecteurs ou choisir un pool de supports indépendant pour chaque lecteur.
10. Cliquez sur le bouton **Avancé**. Dans l'onglet **Paramètres**, sélectionnez l'option **Utiliser accès direct à la bibliothèque**.

    Ne sélectionnez PAS l'option **Utiliser accès direct à la bibliothèque** si vous voulez qu'un seul système envoie des commandes de contrôle de robot pour lancer Data Protector. Le système client que vous avez sélectionné lors de la configuration de la bibliothèque/des lecteurs avec Data Protector contrôlera le robot de la bibliothèque.
11. Cette étape n'est *pas* requise pour les lecteurs MultiPath. Cliquez sur **Suivant**.
    - Si Data Protector est la seule application qui accède au lecteur, cliquez sur l'onglet **Autre**, sélectionnez l'option **Utiliser nom verrouillage**, puis saisissez un nom. Mémorisez le nom car vous en aurez besoin lors de la configuration de ce même lecteur sur un autre client. Il est recommandé d'utiliser l'appellation suivante :

      `LibraryLogicalName_DriveIndex`, par exemple SAN_LIB_D2
    - Si Data Protector n'est pas la seule application qui accède au lecteur, sélectionnez l'option **Utiliser nom verrouillage**, et vérifiez que les règles opérationnelles fournissent un accès exclusif à tous les périphériques à partir d'une seule application à la fois.

- Si le lecteur est utilisé par un seul système, ne sélectionnez PAS l'option **Utiliser nom verrouillage**.

12. Le cas échéant, vous pouvez aussi sélectionner **Le périphérique peut être utilisé pour la restauration** et/ou **Le périphérique peut être utilisé comme source pour la copie d'objets** et indiquer une **balise de périphérique**.
13. Cliquez sur **Terminer** pour quitter l'assistant.

Le lecteur est utilisé par plusieurs systèmes et plusieurs applications (pas seulement par Data Protector) Utilisez le verrouillage de périphérique (définissez un nom de verrouillage) et vérifiez que les règles opérationnelles fournissent un accès exclusif à tous les périphériques à partir d'une seule application à la fois

Le nom du lecteur s'affiche dans la liste des lecteurs configurés. Vous pouvez analyser les lecteurs pour en vérifier la configuration.

Configuration du fichier libtab dans l'environnement SAN

L'objet des fichiers `libtab`est le mappage de l'accès au contrôle du robot de bibliothèque afin de travailler également sur le "système demandant l'accès direct", le chemin d'accès au contrôle local risquant ici d'être différent de celui utilisé sur le système de contrôle du robot de bibliothèque par défaut.

Un fichier `libtab` doit être placé sur chaque client Windows ou UNIX ayant besoin d'un accès direct au robot de bibliothèque et qui est différent du système de contrôle robotique configuré par défaut.

Procédure

1. Créez le fichier `libtab` dans un format texte brut, sur chaque système demandant l'accès direct, dans le répertoire suivant :

   Systèmes Windows : *répertoire_Data_Protector*`\libtab`

   Systèmes HP-UX et Solaris : `/opt/omni/.libtab`

   Autres systèmes UNIX : `/usr/omni/.libtab`
2. Fournissez les informations suivantes dans le fichier `libtab` :

   FullyQualifiedHostname DeviceFile | SCSIPath DeviceName

   - Le *FullyQualifiedHostname* est le nom du client demandant l'accès direct au contrôle du robot de bibliothèque. Si le client fait partie d'un cluster, utilisez le nom du noeud.
   - Le *DeviceFile | SCSIPath* est le chemin de contrôle du pilote du robot de bibliothèque sur ce client.
   - Le *DeviceName* est le nom de la définition du périphérique utilisé sur ce client.

   Vous devez utiliser une ligne par périphérique pour lequel vous demandez l'accès direct.

Si le système fait partie d'un cluster, le *FullyQualifiedHostname* doit être le nom du serveur virtuel et le *DeviceFile | SCSIPath* doit faire référence au noeud cluster (système physique).

Configuration d'un périphérique de bibliothèque DAS ADIC/GRAU

Data Protector propose une stratégie de bibliothèque ADIC/GRAU dédiée, utilisée pour configurer une bibliothèque ADIC/GRAU comme un périphérique de sauvegarde Data Protector.

Chaque système sur lequel vous installez un logiciel d'agent de support et qui accède au robot de la bibliothèque via le serveur DAS est appelé un client DAS.

Les points suivants peuvent contenir des informations supplémentaires :

- La fonctionnalité ADIC/GRAU fait l'objet de licences Data Protector particulières. Pour plus de détails, reportez-vous à *Guide d'installation HPE Data Protector*.
- Etant donné que cette bibliothèque gère des supports utilisés par différentes applications, vous devez indiquer les supports et les lecteurs que vous souhaitez utiliser avec Data Protector et préciser les supports que vous voulez surveiller.
- Data Protector gère sa propre stratégie d'allocation de supports et n'utilise pas de pools scratchés.

Etapes de la configuration

1. Connexion de lecteurs de bibliothèque
2. Préparation de l'installation d'un Agent de support
3. Installation d'un Agent de support
4. Configuration du périphérique de bibliothèque DAS ADIC/GRAU
5. Configuration d'un lecteur dans le périphérique de bibliothèque DAS ADIC/GRAU

Connexion de lecteurs de bibliothèque

Procédure

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

   Pour plus d'informations sur la connexion physique d'un périphérique de sauvegarde à des systèmes UNIX et Windows, reportez-vous au document *Guide d'installation HPE Data Protector*.
2. Configurez la bibliothèque ADIC/GRAU. Consultez la documentation fournie avec la bibliothèque ADIC/GRAU pour obtenir des instructions.

   Pour plus d'informations sur les bibliothèques ADIC/GRAU prises en charge, consultez la page https://softwaresupport.hpe.com/ .

Préparation de l'installation d'un Agent de support

Procédure

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.

   Dans ce fichier, une liste de tous les clients DAS doit être définie. Pour Data Protector, cela signifie que chaque client Data Protector sur lequel un Agent de support est installé doit être défini.

   Chaque client DAS est identifié par un nom de client unique (sans espace), par exemple `OMNIBACK_C1`. Dans cet exemple, le contenu du fichier `C:\DAS\ETC\CONFIG` devrait ressembler à ceci :

   ```
   client client_name = OMNIBACK_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))
   ```

   Ces noms doivent être configurés sur chaque client Agent de support Data Protector comme l'option `omnirc DAS_CLIENT`. Le fichier `omnirc` correspond au fichier `omnirc` dans le répertoire *`répertoire_Data_Protector`* (systèmes Windows), ou au fichier `.omnirc` (systèmes UNIX). Par exemple, sur le système avec l'adresse IP 19.18.17.15, la ligne appropriée dans le fichier `omnirc` est `DAS_CLIENT=OMNIBACK_C1`.
2. Vérifiez comment votre stratégie d'allocation des emplacements de la bibliothèque ADIC/GRAU a été configurée (statique ou dynamique). Consultez le `AMU Reference Manual` pour plus d'informations sur la façon de vérifier le type de stratégie d'allocation utilisée.

   Dans une stratégie statique, un emplacement est dédié à chaque volser, alors que la stratégie d'allocation dynamique attribue les emplacements de façon aléatoire. Configurez Data Protector en fonction de la stratégie qui a été définie.

   Si la stratégie d'allocation statique a été configurée, ajoutez l'option suivante `omnirc` à votre système contrôlant le robot de la bibliothèque :

   ```
   OB2_ACIEJECTTOTAL = 0
   ```

   Notez que cette procédure s'applique à HP-UX et à Windows.

   Contactez le support ADIC/GRAU ou consultez la documentation ADIC/GRAU si vous avez d'autres questions sur la configuration de votre bibliothèque ADIC/GRAU.

Installation d'un Agent de support

Vous pouvez installer soit l'Agent de support général, soit l'Agent de support NDMP sur les systèmes qui seront connectés physiquement à un lecteur de sauvegarde dans une bibliothèque ADIC/GRAU et sur le système qui accédera au robot de la bibliothèque par l'intermédiaire du serveur DAS.

> **REMARQUE :**
> Vous devez disposer de licences spéciales, selon la taille du référentiel des supports ou le nombre de lecteurs et d'emplacements utilisés dans la bibliothèque ADIC/GRAU. Pour plus d'informations, reportez-vous à la section *Guide d'installation HPE Data Protector*.

Conditions préalables

- La bibliothèque ADIC/GRAU doit être configurée et en cours d'exécution. Pour en savoir plus sur la configuration d'une bibliothèque ADIC/GRAU, consultez la documentation livrée avec la bibliothèque.
- Le serveur DAS doit être opérationnel et les clients DAS doivent être correctement configurés.

  Le logiciel DAS doit contrôler la bibliothèque ADIC/GRAU. Il se compose d'un serveur DAS et de plusieurs clients DAS. Pour plus d'informations sur le logiciel DAS, consultez la documentation fournie avec la bibliothèque ADIC/GRAU.
- Recueillez les informations suivantes avant d'installer L'Agent de support :
  - Le nom d'hôte du serveur DAS.
  - Une liste des lecteurs disponibles avec le nom DAS correspondant du lecteur.

    Si vous avez défini le client DAS pour votre système ADIC/GRAU, exécutez les commandes suivantes pour obtenir cette liste :

    `dasadmin listd2 [client]` ou

    `dasadmin listd [client]`, où `[client]` est le client DAS dont les lecteurs réservés doivent être affichés.

    La commande `dasadmin` est située dans le répertoire `C:\DAS\BIN` sur l'hôte OS/2, ou dans le répertoire dans lequel le client DAS a été installé :

    Systèmes Windows : *`%SystemRoot%`*`\system32`

    Systèmes UNIX : `/usr/local/aci/bin`
  - Une liste des zones d'insertion/éjection avec les spécifications de format correspondantes.

    Vous pouvez obtenir cette liste dans la configuration graphique de l'AMS (AML Management Software) sur l'hôte OS/2 :

    Dans le menu Admin, cliquez sur **Configuration** pour lancer la configuration. Double-cliquez sur **I/O** (E/S) pour ouvrir la fenêtre EIF-Configuration, puis cliquez sur **Logical Ranges** (Plages logiques). Les zones d'insertion/éjection disponibles sont listées dans la zone de texte.

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

- **Systèmes Windows :** Systèmes Windows : liste des adresses SCSI pour les lecteurs, par exemple, `.scsi4:0:1:0`
- **Systèmes UNIX :** Liste des fichiers de périphérique UNIX des lecteurs.

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

Procédure

1. Distribuez un composant Agent de support aux clients à l'aide du serveur d'installation et de l'interface utilisateur graphique Data Protector.
2. Installez la bibliothèque ADIC/GRAU pour l'interface client.

   Systèmes Windows :

   - 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.)
   - Copiez également ces trois bibliothèques dans le répertoire *%SystemRoot%*`\system32`.
   - Copiez les services `Portinst` et `Portmapper` 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.)
   - Dans le Panneau de configuration, sélectionnez **Outils d'administration**, **Services**, puis démarrez `portinst` pour installer `portmapper`.
   - Redémarrez le client DAS pour démarrer le service `portmapper`.
   - Dans le Panneau de configuration, sélectionnez **Outils d'administration**, **Services** et vérifiez si les services `portmapper` et `rpc` sont exécutés.

   Systèmes HP-UX, Linux et AIX :

   Copiez la bibliothèque partagée `libaci.sl` (systèmes HP-UX), `libaci.so` (systèmes Linux) ou `libaci.o` (systèmes AIX) dans le répertoire `/opt/omni/lib` (systèmes HP-UX et Linux) ou `/usr/omni/lib` (systèmes AIX). Vous devez disposer des autorisations d'accès à ce répertoire. Assurez-vous que la bibliothèque partagée a lu et exécuté les autorisations pour tout le monde (root, groupe et autres). (Les bibliothèques partagées `libaci.sl` et `libaci.o` font partie du logiciel client DAS livré avec la bibliothèque ADIC/GRAU. Vous pouvez les trouver sur le support d'installation.)
3. Une fois le logiciel DAS correctement installé, exécutez la commande `devbra -dev` pour vérifier si les lecteurs de bibliothèque sont reliés correctement à votre système. La commande réside dans le répertoire par défaut des commandes administratives Data Protector.

   La liste des lecteurs de bibliothèque et de leurs fichiers de périphérique/adresses SCSI correspondant(e)s apparaît.

Configuration du périphérique de bibliothèque DAS ADIC/GRAU

Lorsque la bibliothèque ADIC/GRAU est physiquement connectée au système et qu'un Agent de support est installé, vous pouvez configurer le périphérique de bibliothèque ADIC/GRAU à partir de l'interface utilisateur graphique Data Protector. Le client DAS accède ensuite au robot ADIC/GRAU pendant certaines opérations de gestion des supports (interrogation, insertion, éjection).

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques** puis cliquez sur **Ajouter périphérique**.
3. Dans la zone de texte Nom de périphérique, indiquez le nom du périphérique.
4. Dans la zone de texte Description, indiquez éventuellement une description.
5. Vous pouvez également sélectionner **Périphérique MultiPath**.
6. Dans la liste Type de périphérique, sélectionnez **Bibliothèque DAS GRAU**.
7. Si l'option **Périphérique MultiPath** n'est pas activée, sélectionnez le nom du client Agent de support qui accédera au robot ADIC/GRAU.
8. Dans la zone de texte relative à l'adresse **URL de la console de gestion**, entrez une URL valide pour la console de gestion de bibliothèque (facultatif).
9. Cliquez sur **Suivant**.
10. Dans la zone de texte Serveur DAS, entrez le nom d'hôte du serveur DAS.

    Pour les périphériques MultiPath, sélectionnez également le nom du client et cliquez sur **Ajouter** pour ajouter le chemin d'accès à la liste des chemins configurés.
11. Dans la liste **Comportement en cas de lecteur occupé**, sélectionnez l'action que Data Protector doit effectuer si le lecteur est occupé, puis cliquez sur **Suivant**.
12. Indiquez les zones d'importation et d'exportation pour la bibliothèque et cliquez sur **Ajouter**. Cliquez sur **Suivant**.
13. Dans la liste Type de support, sélectionnez le type de support approprié pour le périphérique.
14. Cliquez sur **Terminer** pour quitter l'assistant Il vous est alors demandé de configurer un lecteur de bibliothèque. Cliquez sur **Oui** pour afficher l'assistant de configuration.

Configuration d'un lecteur dans le périphérique de bibliothèque DAS ADIC/GRAU

Procédure

1. Dans la zone de texte Nom de périphérique, indiquez le nom du lecteur.
2. Dans la zone de texte Description, indiquez éventuellement une description.
3. Vous pouvez également sélectionner **Périphérique MultiPath**.
4. Si l'option **Périphérique MultiPath** n'est pas activée, sélectionnez le nom du client Agent de

support qui accédera au robot ADIC/GRAU.

5. Cliquez sur **Suivant**.
6. Dans la zone de texte Lecteur de données, spécifiez l'adresse SCSI du périphérique.

   Pour les périphériques MultiPath, sélectionnez également le nom du client Agent de support qui accédera au robot ADIC/GRAU et cliquez sur Ajouter pour ajouter le chemin d'accès à la liste des chemins configurés.
7. Sélectionnez l'option **Découvrir automatiquement adresse SCSI modifiée** pour activer la détection automatique des adresses SCSI modifiées.
8. Dans la zone de texte Nom du lecteur, spécifiez le nom du lecteur ADIC/GRAU que vous avez obtenu lors de l'installation d'un Agent de support. Cliquez sur **Suivant**.
9. Sélectionnez le **Pool de supports par défaut** pour le lecteur.
10. Cliquez sur **Avancé** pour définir des options avancées pour le lecteur, comme la **Simultanéité**. Cliquez sur **OK**. Cliquez sur **Suivant**.
11. Le cas échéant, vous pouvez aussi sélectionner **Le périphérique peut être utilisé pour la restauration** et/ou **Le périphérique peut être utilisé comme source pour la copie d'objets** et indiquer une **balise de périphérique**.
12. Cliquez sur **Terminer** pour quitter l'assistant

Configuration d'un périphérique de bibliothèque ACS StorageTek

Data Protector propose une stratégie de bibliothèque ACS StorageTek dédiée, utilisée pour configurer une bibliothèque ACS StorageTek comme un périphérique de sauvegarde Data Protector.

Chaque système sur lequel vous installez un logiciel d'agent de support et qui accède au robot de la bibliothèque via ACSLC est appelé un client ACS.

Les points suivants peuvent contenir des informations supplémentaires :

- La fonctionnalité STK fait l'objet de licences Data Protector particulières. Consultez le *Guide d'installation HPE Data Protector* pour plus de détails.
- Etant donné que cette bibliothèque gère des supports utilisés par différentes applications, vous devez indiquer les supports et les lecteurs que vous souhaitez utiliser avec Data Protector et préciser les supports que vous voulez surveiller.
- Data Protector gère sa propre stratégie d'allocation de supports et n'utilise pas de pools scratchés.

Etapes de la configuration

1. Connexion de lecteurs de bibliothèque
2. Installation d'un Agent de support
3. Configuration du périphérique de bibliothèque ACS StorageTek
4. Configuration d'un lecteur dans le périphérique de bibliothèque ACS StorageTek

Connexion de lecteurs de bibliothèque

Procédure

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

   Pour plus d'informations sur la connexion physique d'un périphérique de sauvegarde à des systèmes UNIX et Windows, reportez-vous au document *Guide d'installation HPE Data Protector*.
2. Configurez la bibliothèque ACS StorageTek. Consultez la documentation fournie avec la bibliothèque pour obtenir des instructions.

   Pour plus d'informations sur les bibliothèques StorageTek prises en charge, consultez la page https://softwaresupport.hpe.com/.

Installation d'un Agent de support

Vous pouvez installer soit l'Agent de support général, soit l'Agent de support NDMP sur les systèmes qui seront connectés physiquement à un lecteur de sauvegarde dans une bibliothèque StorageTek et sur le système qui accédera au robot de la bibliothèque par l'intermédiaire de l'ACSLS.

> **REMARQUE :**
> Vous devez disposer de licences spéciales, selon la taille du référentiel des supports ou le nombre de lecteurs et d'emplacements utilisés dans la bibliothèque StorageTek. Pour plus d'informations, voir *Guide d'installation HPE Data Protector*.

Conditions préalables

- La bibliothèque StorageTek doit être configurée et en cours d'exécution. Pour en savoir plus sur la configuration d'une bibliothèque StorageTek, consultez la documentation livrée avec la bibliothèque.
- Vous devez obtenir les informations suivantes avant de commencer à installer le logiciel Agent de support :
  - Le *hostname* 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. 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)
    ```
  - 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
```

- 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)
  ```

- 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
  ```

- **Systèmes Windows :** Systèmes Windows : liste des adresses SCSI pour les lecteurs, par exemple, `.scsi4:0:1:0`

- **Systèmes UNIX :** Liste des fichiers de périphérique UNIX des lecteurs.

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

Procédure

1. Distribuez le composant Agent de support aux clients à l'aide du serveur d'installation pour Windows et de l'interface utilisateur graphique Data Protector.
2. Démarrez le démon `ssi` ACS sur tous les hôtes de la bibliothèque (Clients de l'Agent de support) avec accès au robot de bibliothèque.

   Systèmes Windows :

   Installez le service `LibAttach`. Pour plus de détails à ce sujet, reportez-vous à 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.

   > **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 ce service, consultez la documentation fournie avec la bibliothèque StorageTek.

Systèmes HP-UX et Solaris :

Exécuter la commande suivante :

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

Systèmes AIX :

Exécuter la commande suivante :

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

3. À partir du répertoire de commandes administratives Data Protector par défaut, exécutez la commande `devbra -dev` pour vérifier si les lecteurs de bibliothèque sont reliés correctement à vos clients Agent de support.

   La liste des lecteurs de bibliothèque et de leurs fichiers de périphérique/adresses SCSI correspondant(e)s apparaît.

Configuration du périphérique de bibliothèque ACS StorageTek

Lorsque la bibliothèque StorageTek est physiquement connectée au système et qu'un Agent de support est installé, vous pouvez configurer le périphérique de bibliothèque StorageTek à partir de l'interface utilisateur graphique Data Protector. Le client ACS accède ensuite au robot StorageTek pendant certaines opérations de gestion des supports (interrogation, insertion, éjection).

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques** puis cliquez sur **Ajouter périphérique**.
3. Dans la zone de texte Nom de périphérique, indiquez le nom du périphérique.
4. Dans la zone de texte Description, indiquez éventuellement une description.
5. Vous pouvez également sélectionner **Périphérique MultiPath**.
6. Dans la liste Type de périphérique, sélectionnez **Bibliothèque ACS StorageTek**.
7. Si l'option **Périphérique MultiPath** n'est pas activée, sélectionnez le client Agent de support qui accédera au robot StorageTek.
8. Dans la zone de texte relative à l'adresse **URL de la console de gestion**, entrez une URL valide pour la console de gestion de bibliothèque (facultatif).
9. Cliquez sur **Suivant**.
10. Dans la zone de texte Nom d'hôte ACSLM, entrez le nom d'hôte du serveur ACS.

    Pour les périphériques MultiPath, sélectionnez également le nom du client et ajoutez le chemin d'accès à la liste des chemins configurés.
11. Dans la liste **Comportement en cas de lecteur occupé**, sélectionnez l'action que Data Protector doit effectuer si le lecteur est occupé, puis cliquez sur **Suivant**.
12. Indiquez les **CAP** pour la bibliothèque et cliquez sur **Ajouter**. Cliquez sur **Suivant**.
13. Dans la liste Type de support, sélectionnez le type de support approprié pour le périphérique.

14. Cliquez sur **Terminer** pour quitter l'assistant Il vous est alors demandé de configurer un lecteur de bibliothèque. Cliquez sur **Oui** pour afficher l'assistant de configuration.

Configuration d'un lecteur dans le périphérique de bibliothèque ACS StorageTek

Procédure

1. Dans la zone de texte Nom de périphérique, indiquez le nom du lecteur.
2. Dans la zone de texte Description, indiquez éventuellement une description.
3. Vous pouvez également sélectionner **Périphérique MultiPath**.
4. Si l'option **Périphérique MultiPath** n'est pas activée, sélectionnez le client Agent de support qui accédera au robot StorageTek.
5. Cliquez sur **Suivant**.
6. Dans la zone de texte Lecteur de données, spécifiez l'adresse SCSI du périphérique.

   Pour les périphériques MultiPath, sélectionnez également le client Agent de support qui accédera au robot StorageTek et cliquez sur **Ajouter** pour ajouter le chemin d'accès à la liste des chemins configurés.
7. Dans la zone de texte Index de lecteur, spécifiez l'**Index de lecteur** StorageTek que vous avez obtenu lors de l'installation d'un Agent de support. L'index de lecteur est une combinaison de quatre nombres séparés par des virgules. Cliquez sur **Suivant**.
8. Sélectionnez le **Pool de supports par défaut** pour le lecteur.
9. Cliquez sur **Avancé** pour définir des options avancées pour le lecteur, comme la **Simultanéité**. Cliquez sur **OK**. Cliquez sur **Suivant**.
10. Le cas échéant, vous pouvez aussi sélectionner **Le périphérique peut être utilisé pour la restauration** et/ou **Le périphérique peut être utilisé comme source pour la copie d'objets** et indiquer une **balise de périphérique**.
11. Cliquez sur **Terminer** pour quitter l'assistant

À propos de l'utilisation des périphériques de sauvegarde

L'utilisation des périphériques de sauvegarde s'applique à des tâches telles que l'analyse d'un périphérique pour identifier ses supports, le verrouillage d'un périphérique avec indication d'un nom de verrouillage, l'éjection planifiée d'un support, le nettoyage automatique ou manuel de lecteurs encrassés, l'attribution d'un nouveau nom à un périphérique de sauvegarde et la réponse à une demande de montage pour confirmer que le support requis se trouve dans un périphérique.

Data Protector fournit également un ensemble d'options avancées pour les périphériques et les supports, dont la disponibilité dépend du type de périphérique, qui sont utiles à la gestion des périphériques et des supports.

De plus, vous pouvez utiliser plusieurs types de lecteur dans la même bibliothèque, mais vous devez connaître les caractéristiques des supports utilisés.

Lorsqu'un périphérique est inopérant pour une raison quelconque, vous pouvez le désactiver pour la sauvegarde et utiliser automatiquement un autre périphérique disponible dans la liste correspondante.

Si vous ne voulez plus utiliser un périphérique, vous pouvez le supprimer de la configuration Data Protector.

Options avancées des périphériques et des supports

Data Protector fournit un ensemble d'options avancées pour les périphériques et les supports. La disponibilité de ces options dépend du type de périphérique utilisé. Par exemple, davantage d'options sont disponibles pour la configuration d'une bibliothèque que pour celle d'un périphérique autonome.

Vous pouvez faire appel à ces options lors de la configuration d'un nouveau périphérique ou lors de la modification des propriétés du périphérique. Ces options s'appliquent au périphérique correspondant dans son ensemble. Vous pouvez également définir un sous-ensemble d'options pour répondre aux besoins d'une spécification de sauvegarde particulière. Ces dernières prévalent sur les options définies pour le périphérique dans son ensemble. Vous pouvez y accéder lors de la configuration ou de la modification de votre spécification de sauvegarde.

Pour plus d'informations sur les options avancées, reportez-vous au Aide de HPE Data Protector.

Options avancées - Paramètres

Simultanéité

Options

- Contrôle CRC
- Détecter lecteur encrassé
- Cryptage sur lecteur
- Ejecter support après la session
- Nouvelle analyse
- Utiliser accès direct à la bibliothèque (option propre à SAN)

Options avancées - Tailles

- Taille de bloc (Ko)
- Mémoires tampon d'Agent de disque
- Taille de segment (Mo)

Options avancées - Autres

Demande de montage

- Délai (minutes)
- Script

Noms de verrouillage de périphérique

- Utiliser nom verrouillage

Bibliothèque comportant plusieurs types de lecteurs

Une même bibliothèque peut comporter plusieurs types de lecteurs utilisant la même technologie ; par exemple, DLT 4000/7000/8000 (cela est également possible au sein de la famille DDS). Toutefois, des problèmes peuvent se poser si vous souhaitez utiliser indifféremment les supports dans les lecteurs, mais que vous ne vous assurez pas qu'un format commun aux supports est utilisé. Par exemple, lors de la restauration, un DLT-4000 ne peut pas lire une bande qui a été écrite avec un DLT-8000 (densité supérieure). De même, les supports compressés et non compressés ne peuvent pas être interchangés.

Vous pouvez éviter ce type de problème en paramétrant la même densité ou en créant un pool de supports différent pour chaque type de lecteur.

Paramètre de densité identique

Cette méthode fait appel à un format commun pour tous les supports, ce qui permet d'employer indifféremment ces derniers dans tous les lecteurs. Pour les périphériques utilisés sur les systèmes Windows, vous devez consulter la documentation du lecteur pour savoir comment employer une densité d'écriture spécifique. Sur les systèmes UNIX, vous pouvez définir la densité des lecteurs lors de la création du fichier de périphérique ou en sélectionnant les fichiers des périphériques associés et en les utilisant dans les définitions de périphérique. Vous devez définir la même valeur de densité pour les différents périphériques. Si vous avez un DLT 4000 et un DLT 7000, par exemple, la densité définie doit être celle du DLT 4000. Vous devez également vous assurer que le paramètre de taille de bloc est identique pour tous les périphériques. Ce paramètre doit être employé dans la définition de périphérique lors du formatage des supports. Lorsque le paramètre de densité est le même pour tous les supports, vous pouvez utiliser le pool libre comme vous le souhaitez. Au cours de la restauration, les supports et les lecteurs peuvent être utilisés indifféremment.

Un pool de supports différent pour chaque type de lecteur

Cette méthode, qui établit une séparation claire entre les supports utilisés par un groupe de lecteurs et ceux utilisés par un autre groupe, permet d'optimiser l'utilisation des lecteurs et des supports. Vous pouvez configurer des pools de supports séparés pour les différents groupes de lecteurs. Ceci permet d'utiliser des paramètres de densité différents pour chaque type de lecteur. Vous pouvez par exemple, créer un pool "DLT-4000" et un pool "DLT-8000". Ces paramètres doivent être employés dans la définition de périphérique lors du formatage des supports. Les supports du pool "DLT-8000-densité maximale" doivent être formatés par un DLT-8000 avec le paramètre de densité le plus élevé.

Support de pool libre

Vous ne pouvez pas utiliser un pool libre "parmi" de tels pools. Les supports de l'"autre" pool ne seraient alors pas identifiés correctement par les périphériques : ils seraient pris pour des supports étrangers. Le concept de pool libre ne peut être employé *avec un pool* (comme le pool DLT-8000) *pour chaque type de lecteur*, que dans le cas où le même type de support (DLT) est écrit de façon

incompatible. Notez que, lors de la restauration, les supports provenant d'un pool donné ne peuvent être utilisés qu'avec les périphériques associés.

A propos de l'analyse

L'analyse consiste à vérifier le format d'un support inséré dans un lecteur, à afficher le contenu du référentiel du périphérique et à mettre à jour ces informations dans la base de données interne.

- Avec un périphérique autonome, vous analysez un support se trouvant dans le lecteur.
- Avec un périphérique de bibliothèque, vous analysez les supports se trouvant dans les emplacements sélectionnés.
- Avec un périphérique de bibliothèque disposant d'un support de codes-barres, vous analysez le support à l'aide des codes-barres.
- Avec un périphérique de bibliothèque de fichiers, vous mettez à jour les informations dans la base de données interne (IDB) concernant les dépôts de fichier.
- Avec des bibliothèques DAS ADIC/GRAU ou ACS STK, Data Protector interroge un serveur DAS ADIC/GRAU ou ACSLM STK, puis synchronise les informations dans l'IDB en fonction des données renvoyées par le serveur.

Quand effectuer une analyse ?

Vous analysez un périphérique chaque fois que vous voulez mettre à jour les informations de Data Protector relatives aux supports dans le périphérique. Vous devez également l'analyser si vous changez manuellement l'emplacement du support. Le changement manuel de position (emplacement, lecteur) d'un support crée des incohérences avec les informations de la base de données interne, car Data Protector n'a pas eu connaissance du changement effectué. Cette fonction synchronise la MMDB avec les supports qui se trouvent aux positions sélectionnées (emplacements d'une bibliothèque, par exemple).

Vérifiez que tous les supports de votre cellule possèdent des étiquettes de codes-barres uniques. Si un code-barres existant est détecté lors d'une analyse, le support qui se trouve déjà dans la base de données interne est déplacé.

Effectuez l'analyse d'un périphérique de bibliothèque de fichiers si vous avez déplacé l'un des dépôts de fichier.

Limites

L'analyse des volsers peut échouer si la bibliothèque ADIC/GRAU est configurée avec plus de 3970 volsers dans un même référentiel. Pour contourner ce problème, vous pouvez configurer plusieurs bibliothèques ADIC/GRAU logiques afin de diviser les différents emplacements du référentiel en plusieurs petits référentiels.

> **IMPORTANT :**
> Avec les bibliothèques DAS ADIC/GRAU et ACS STK, il n'est pas recommandé d'interroger le serveur DAS ou ACSLM STK lorsque plusieurs bibliothèques logiques sont configurées pour la même bibliothèque physique. Ajoutez les volsers manuellement. Avec les bibliothèques DAS ADIC/GRAU, cependant, lorsque les bibliothèques logiques ne sont pas configurées à l'aide de Data Protector, mais au contraire avec les utilitaires DAS ADIC/GRAU, l'opération de requête

de Data Protector peut être utilisée en toute sécurité sur les bibliothèques.

Nettoyage du lecteur

Data Protector offre plusieurs méthodes de nettoyage des lecteurs encrassés :

- Mécanisme de nettoyage intégré à la bibliothèque

  Certaines bibliothèques à bande disposent d'une fonctionnalité de nettoyage qui se déclenche automatiquement lorsqu'un lecteur demande le nettoyage des têtes. Lorsque la bibliothèque détecte un lecteur encrassé, elle charge automatiquement une bande de nettoyage (Data Protector n'est pas informé de cette action). Cela interrompt et fait échouer toute session active. Cette procédure spécifique de nettoyage par matériel n'est pas recommandée car elle n'est pas compatible avec Data Protector. Utilisez plutôt un nettoyage automatique des lecteurs géré par Data Protector.
- Nettoyage automatique des lecteurs géré par Data Protector

  Data Protector permet le nettoyage automatique de la plupart des périphériques utilisant des bandes de nettoyage. Pour les bibliothèques SCSI et les périphériques de magasin, vous pouvez déterminer les emplacements contenant les bandes nettoyantes. Un lecteur encrasse envoie la demande de nettoyage, puis Data Protector utilise la bande de nettoyage pour nettoyer le lecteur. Cette méthode empêche l'échec des sessions en raison de disques encrassés, à condition que les supports appropriés soient disponibles pour la sauvegarde. Le nettoyage automatique des lecteurs est possible sur les bibliothèques qui prennent en charge ou pas les codes-barres.
- Nettoyage manuel

  Si le nettoyage automatique des lecteurs n'est pas configuré, vous devez nettoyer manuellement le lecteur encrassé. Si Data Protector détecte un lecteur encrassé, une demande de nettoyage apparaît dans la fenêtre du moniteur de session. Vous devez ensuite insérer manuellement une bande de nettoyage dans le lecteur.

Une cartouche de nettoyage spéciale avec une bande légèrement abrasive est utilisée pour nettoyer la tête. Une fois la cartouche chargée, le lecteur la reconnaît et commence le nettoyage de la tête.

Limites

- Data Protector ne prend pas en charge la commande SCSI unique d'un fournisseur de diagnostic pour effectuer le nettoyage de lecteur avec des bandes de nettoyage stockées dans un des emplacements spéciaux de stockage de la bande de nettoyage. Ces emplacements spéciaux de stockage de la bande de nettoyage ne sont pas accessibles à l'aide des commandes SCSI standard, et ne peuvent donc pas être utilisés avec le nettoyage automatique des lecteurs géré par Data Protector. Configurez les emplacements standard pour le stockage des bandes de nettoyage.
- La détection et l'utilisation de bandes de nettoyage varient selon la plate-forme système sur laquelle un Agent de support est en cours d'exécution. Pour plus d'informations, reportez-vous au *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*.
- Vous ne devriez pas utiliser un autre type d'application de gestion de périphérique si vous configurez un nettoyage automatique des lecteurs géré par Data Protector car cela peut entraîner des résultats inattendus. Cela est dû au fait que la demande `cleanme` est effacée dès sa lecture, en fonction du type de périphérique spécifique et du fournisseur.
- Le nettoyage automatique des lecteurs pour les bibliothèques logiques avec une bande de nettoyage

partagée n'est pas pris en charge. Chaque bibliothèque logique doit avoir sa bande de nettoyage spécifique configurée.

Conditions du nettoyage automatique

- Dans les bibliothèques qui ne prennent pas en charge les codes-barres, un emplacement pour bande de nettoyage a été configuré dans la définition du périphérique Data Protector et contient une cartouche à bande de nettoyage. L'emplacement pour bande de nettoyage doit être configuré avec les autres emplacements de la bibliothèque.
- Dans les bibliothèques prenant en charge les codes-barres, cette prise en charge des codes-barres doit être activée pour permettre le nettoyage automatique des lecteurs. Les bandes de nettoyage possèdent une étiquette à code-barres portant le préfixe `CLN`, permettant à Data Protector de reconnaître automatiquement les codes-barres des bandes de nettoyage.
- Pour le périphérique configuré, l'option Détecter lecteur encrassé est activée.

Lorsque Data Protector reçoit la notification que le lecteur doit être nettoyé, il charge automatiquement la bande de nettoyage, nettoie le lecteur, puis reprend la session. Toutes les activités de nettoyage sont enregistrées dans le fichier `cleaning.log` situé dans le répertoire des fichiers journaux du serveur Data Protector.

Éjection de support planifiée

Data Protector permet de planifier l'éjection des supports en utilisant la fonction de génération de rapports couplée à un script.

Il faut créer un programme ou script sur le Gestionnaire de cellule pour effectuer l'éjection et y installer tout interprète requis.

Vous pouvez configurer et planifier un groupe de rapports pour qu'un rapport soit créé et envoyé à un script. Un tel groupe de rapports doit inclure un rapport comportant la liste des supports à éjecter (vous pouvez utiliser le rapport Liste des supports, par exemple). Lorsque le groupe de rapports est lancé (suite à une planification ou à une notification, par exemple, celle de la fin d'une session), Data Protector lance le script avec le résultat du rapport comme entrée. Le script analyse le rapport et déclenche l'éjection du support indiqué à l'aide de la commande CLI Data Protector `omnimm`.

Par défaut, dans l'observateur de journal d'événements, un message vous indique si vous devez enlever des supports de leurs logements de bande pour que l'éjection puisse continuer (par exemple, si le nombre de supports à éjecter est supérieur au nombre de logements de bande vides dans une bibliothèque). Si vous n'enlevez pas de supports des logements de bande au bout d'un laps de temps défini par défaut et qu'il reste des supports à éjecter, la commande `omnimm` abandonne l'opération. Vous pouvez modifier ce délai par défaut dans le fichier `omnirc`.

Verrouillage de périphériques

Vous pouvez configurer plusieurs fois le même périphérique physique avec des caractéristiques différentes en le configurant simplement avec des noms de périphérique différents. Il est ainsi possible de configurer un périphérique physique en plusieurs périphériques de sauvegarde Data Protector et de l'utiliser pour plusieurs sessions de sauvegarde. Le verrouillage interne des périphériques logiques empêche deux sessions Data Protector d'accéder simultanément au même périphérique physique. Par

exemple, si une session de sauvegarde utilise un périphérique donné, toutes les autres sessions de sauvegarde/restauration doivent attendre que ce périphérique soit disponible avant de commencer à l'utiliser. Lorsqu'une session de sauvegarde ou de restauration démarre, Data Protector verrouille le périphérique, le lecteur et l'emplacement utilisés pour la session.

Les sessions qui exécutent des opérations sur les supports, telles qu'une initialisation, une analyse, une vérification, une copie ou une importation, verrouillent également les périphériques. Pendant ce temps, aucune autre opération ne peut verrouiller et utiliser le périphérique. Si une session de support ne peut pas obtenir de verrouillage, l'opération échoue et vous devez relancer l'opération ultérieurement.

Lorsqu'une session de sauvegarde ou de restauration génère une demande de montage, le verrouillage est annulé, afin que vous puissiez effectuer uniquement des opérations de gestion de supports. Le périphérique reste réservé afin qu'aucune autre session de sauvegarde ou de restauration ne puisse l'utiliser. De plus, aucune autre opération de gestion de supports n'est autorisée sur le même lecteur pendant la première opération. Lorsque la demande de montage est confirmée, la session de sauvegarde ou de restauration verrouille de nouveau le périphérique et poursuit la session.

Le verrouillage interne agit sur les périphériques logiques plutôt que sur les périphériques physiques. Il existe donc un risque de conflit si vous indiquez un nom de périphérique donné dans une spécification de sauvegarde, et un autre nom pour le même périphérique physique dans une autre spécification. En fonction de la planification de sauvegarde, Data Protector peut tenter d'utiliser simultanément le même périphérique physique pour plusieurs sessions de sauvegarde, ce qui risque d'entraîner un conflit. Ceci peut également se produire si deux noms de périphérique sont utilisés dans d'autres opérations (par exemple, sauvegarde et restauration ou sauvegarde et analyse). Pour éviter tout conflit lorsque Data Protector tente d'utiliser simultanément le même périphérique physique au cours de plusieurs sessions de sauvegarde, indiquez un nom de verrouillage virtuel dans les configurations de périphérique. Data Protector utilise alors ce nom de verrouillage pour vérifier la disponibilité du périphérique et éviter ainsi les conflits. Vous devez utiliser le même nom de verrouillage dans toutes les configurations de périphérique de sauvegarde du même périphérique physique.

> **REMARQUE :**
> Les informations concernant un périphérique physique figurant dans le rapport sur le flux du périphérique sont prélevées sur le périphérique actuellement configuré et peuvent différer de ce qu'elles étaient au moment où le périphérique a été effectivement utilisé (par exemple, le nom logique du périphérique a été récemment changé, mais certaines sessions de la base de données interne contiennent toujours l'ancien nom).
>
> Le rapport sur le flux du périphérique affiche toujours les informations actuelles, à savoir la représentation physique actuelle et le nom de périphérique logique en vigueur.

Désactivation d'un périphérique de sauvegarde

Désactivation manuelle d'un périphérique de sauvegarde

Si vous désactivez un périphérique de sauvegarde, il sera ignoré lors de toutes les sauvegardes ultérieures. Le périphérique disponible suivant, défini dans la liste de périphériques pour la spécification de sauvegarde, est alors utilisé, à condition que le partage de charge ait été sélectionné. Tous les périphériques utilisant le même nom de verrouillage que celui qui est désactivé le sont également.

Ceci permet d'éviter l'échec d'une sauvegarde si un périphérique est endommagé ou se trouve en mode de maintenance, car d'autres périphériques sont disponibles (et configurés) pour la sauvegarde.

La désactivation d'un périphérique de sauvegarde est utile si le périphérique est endommagé ou en mode maintenance.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**. La liste des périphériques configurés s'affiche dans la zone de résultats.
3. Cliquez avec le bouton droit de la souris sur le périphérique à désactiver, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Paramètres**, puis sélectionnez l'option **Désactiver périphérique**.
5. Cliquez sur **Appliquer**.

Le périphérique est alors désactivé. Pour activer le périphérique pour la sauvegarde, désélectionnez l'option **Désactiver périphérique**.

Désactivation automatique d'un périphérique de sauvegarde

Vous pouvez configurer Data Protector de telle sorte qu'il désactive les périphériques sur lesquels un certain nombre d'erreurs inconnues ont été détectées. Vous fixez la valeur de seuil en définissant l'option globale `SmDeviceErrorThreshold` sur `SmDeviceErrorThreshold=MaxNumberOfUnknownErrors`.

Pour activer la sauvegarde du périphérique une fois cette valeur fixée, cliquez sur celui-ci avec le bouton droit sur le périphérique et sélectionnez **Activer périphérique**.

Attribution d'un nouveau nom à un périphérique de sauvegarde

Lorsque vous attribuez un nouveau nom à un périphérique de sauvegarde, ce dernier ne sera plus utilisé sous son nom précédent pour effectuer une sauvegarde ou une restauration.

> **IMPORTANT :**
> N'oubliez pas de supprimer le nom précédent du périphérique de toutes les spécifications de sauvegarde dans lesquelles il a été utilisé. Sinon, Data Protector tente de sauvegarder ou de restaurer à partir d'un périphérique qui n'existe pas, et la session échoue.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**. La liste des périphériques configurés s'affiche dans la zone de résultats.
3. Cliquez avec le bouton droit sur le nom du périphérique, puis cliquez sur Propriétés.
4. Dans la page de propriétés Général, modifiez le nom du périphérique dans la zone de texte

correspondante.

5. Cliquez sur **Appliquer**.

Le périphérique s'affiche alors sous son nouveau nom dans la liste des périphériques configurés.

Suppression d'un périphérique de sauvegarde

Lorsque vous supprimez un périphérique de sauvegarde de la configuration Data Protector, celui-ci n'est plus utilisé pour les opérations de sauvegarde ou de restauration.

> **IMPORTANT :**
> N'oubliez pas de supprimer le nom précédent du périphérique de toutes les spécifications de sauvegarde dans lesquelles il a été utilisé. Sinon, Data Protector tente de sauvegarder ou de restaurer à partir d'un périphérique qui n'existe pas, et la session échoue.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**. La liste des périphériques configurés s'affiche dans la zone de résultats.
3. Cliquez avec le bouton droit sur le périphérique à supprimer, puis cliquez sur Supprimer. Confirmez l'opération.

Le périphérique est alors supprimé de la liste des périphériques configurés.

> **CONSEIL :**
> Si vous n'utilisez plus un périphérique de sauvegarde avec Data Protector, vous pouvez supprimer le composant logiciel Agent de support du système. Ceci peut être réalisé à l'aide du contexte Client.

Réponse aux demandes de montage

Vous répondez à une demande de montage pour confirmer que le support requis se trouve dans un périphérique. Vous devez être attentif à la façon dont les supports sont sélectionnés pour la sauvegarde.

Conditions préalables

Vous devez faire partie du groupe d'utilisateurs Admin ou disposer des droits d'utilisateur Moniteur.

Procédure

1. Dans la liste de contexte, sélectionnez **Moniteur**.
2. Insérez le support requis dans le périphérique. Si vous utilisez un périphérique de bibliothèque, il n'est pas nécessaire d'utiliser l'emplacement requis par la demande de montage.
3. Dans la zone de résultats, cliquez deux fois sur la session en demande de montage pour afficher les informations sur la session.

4. Sélectionnez le périphérique en demande de montage.
5. Dans le menu **Actions**, sélectionnez **Confirmer demande de montage**, ou cliquez avec le bouton droit sur le périphérique en demande de montage, puis choisissez **Confirmer demande de montage**.

L'état de la session et du périphérique devient En cours d'exécution.

À propos des réseaux SAN (Storage Area Network)

Qu'est-ce qu'un réseau SAN ?

Le système Storage Area Network (SAN) est un réseau dédié au stockage de données, qui repose sur la technologie haut débit Fibre Channel. Le réseau SAN permet de décharger le stockage de serveurs d'applications vers un réseau distinct. Data Protector prend en charge cette technologie en permettant à plusieurs hôtes de partager des périphériques de stockage connectés via un SAN, établissant ainsi une connectivité entre plusieurs systèmes et plusieurs périphériques. Cette opération s'effectue en définissant le même périphérique plusieurs fois, par exemple une fois sur chaque système qui a besoin d'accéder au périphérique.

Lors de l'utilisation de Data Protector dans l'environnement SAN, vous devez considérer les points suivants :

- Chaque système peut avoir son propre périphérique local (pseudo), bien que les périphériques soient généralement partagés entre plusieurs systèmes. Cela s'applique aussi bien aux lecteurs individuels qu'aux robots des bibliothèques.
- Vous devez éviter que plusieurs systèmes écrivent simultanément sur le même périphérique. L'accès aux périphériques doit être synchronisé entre tous les systèmes. Pour cela, utilisez des mécanismes de verrouillage.
- La technologie SAN offre un excellent moyen de gérer les robots de la bibliothèque à partir de plusieurs systèmes. Cela permet de gérer directement les robots, à condition que les demandes qui leur sont adressées soient synchronisées entre tous les systèmes concernés.

FC-AL et LIP

L'utilisation de périphériques à bande dans des boucles Fibre Channel Arbitrated Loops (FC-AL) peut provoquer certaines anomalies qui risquent d'interrompre une session de sauvegarde. Le problème vient du fait que la boucle FC-AL effectue un protocole d'initialisation de boucle (Loop Initialization Protocol ou LIP) chaque fois qu'un nouveau lien FC est connecté/déconnecté, et chaque fois qu'un système relié à la boucle FC-AL est redémarré. Cette réinitialisation de la boucle FC-AL provoque l'arrêt des sauvegardes en cours. Ces tâches terminées doivent être redémarrées.

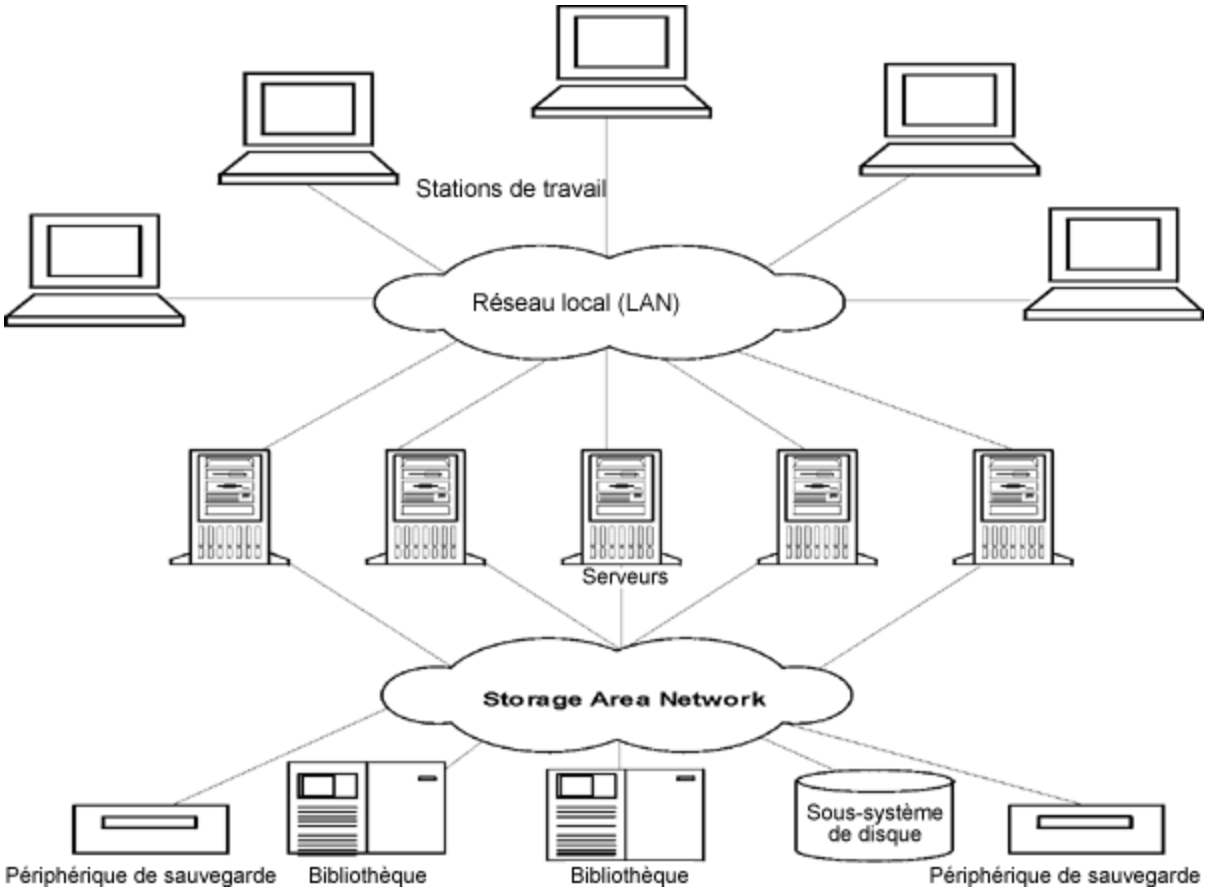
Quand un protocole LIP se produit sur la boucle FC-AL, tout utilitaire avec un processus d'E/S actif affiche une erreur d'E/S. Pour les utilitaires de sauvegarde qui tentent d'utiliser une bande partagée, une erreur d'E/S entraîne l'échec de la session de sauvegarde en cours :

- Les bandes sont rembobinées et déchargées
- La session de sauvegarde est abandonnée

La procédure suivante est recommandée :

- N'ajoutez ou ne supprimez aucun périphérique de la boucle AL lorsque des sessions de sauvegarde sont en cours.
- Ne touchez pas les composants FC lorsque des sessions de sauvegarde sont en cours. La charge statique peut provoquer une LIP.
- N'utilisez pas `discovery` sur Windows ou `ioscan` sur un système HP-UX car cela peut également entraîner une LIP.

Exemple de connectivité entre plusieurs systèmes et plusieurs périphériques dans un environnement SAN



Verrouillage de périphériques dans l'environnement SAN

Data Protector prend en charge le concept SAN dans la mesure où il permet à plusieurs systèmes de partager des périphériques de sauvegarde dans l'environnement SAN. Le même périphérique peut être partagé par plusieurs applications. Il peut également être partagé par plusieurs systèmes dans l'environnement Data Protector. Le but du verrouillage est de faire en sorte qu'un seul système à la fois communique avec un périphérique partagé entre plusieurs systèmes.

Verrouillage de périphériques utilisés exclusivement par Data Protector

Si Data Protector est la seule application qui utilise un lecteur, mais que plusieurs systèmes souhaitent accéder à ce lecteur, vous pouvez utiliser le mécanisme de verrouillage de périphérique.

Si Data Protector est la seule application utilisant le contrôle robotique à partir de plusieurs systèmes, Data Protector gère la procédure en interne à condition que le contrôle de bibliothèque se trouve dans la même cellule que tous les systèmes devant la contrôler. Dans ce cas, la synchronisation des accès est gérée par le contrôle interne Data Protector.

Verrouillage de périphériques utilisés par plusieurs applications

Si plusieurs systèmes utilisent Data Protector pour accéder au même périphérique physique, le mécanisme de verrouillage de périphérique doit être utilisé.

Si Data Protector et au moins une autre application ont besoin d'utiliser le même périphérique à partir de plusieurs systèmes, le même mécanisme de verrouillage de périphérique (générique) doit être utilisé par chaque application. Ce mécanisme doit fonctionner avec plusieurs applications. Ce mode n'est actuellement pas pris en charge par Data Protector. En cas de nécessité, des règles de fonctionnement doivent assurer l'accès exclusif à tous les périphériques d'une application à la fois.

Accès direct et indirect à la bibliothèque

Lorsque vous configuriez Data Protector avec un dispositif de bibliothèque SCSI ou des bibliothèques silo (ADIC/GRAU et StorageTek), il y a deux manières pour les systèmes client d'accéder à la robotique de bibliothèque :

Accès indirect à la bibliothèque

Avec l'accès indirect à la bibliothèque, seul un système (le système de contrôle robotique par défaut) envoie les commandes robotiques lancées à partir de Data Protector. Tout autre système demandant une fonction robotique envoie sa requête au système de contrôle robotique, qui envoie ensuite la commande en question au robot. Cette opération est effectuée de manière transparente dans Data Protector pour toutes les demandes émanant de Data Protector.

Accès direct à la bibliothèque

Avec l'accès direct à la bibliothèque, chaque système envoie directement des commandes de contrôle au robot de bibliothèque. Ainsi, aucun système ne dépend d'autres systèmes pour pouvoir fonctionner.

Avec l'accès direct à la bibliothèque et l'envoi de commandes par plusieurs systèmes, il est nécessaire de coordonner la séquence de cette communication.

Dans Data Protector, chaque définition de bibliothèque est associée à un hôte contrôlant le robot de bibliothèque (par défaut). Si un autre hôte demande le déplacement d'un support, Data Protector accède tout d'abord au système spécifié dans la définition de la bibliothèque pour effectuer ce déplacement. Si le système n'est pas disponible, un accès direct à partir de l'host local à la robotique

de la bibliothèque peut être utilisé si le fichier `libtab` est déterminé. Tout cela est effectué de manière transparente dans Data Protector.

Si l'accès direct à la bibliothèque est activé pour les périphériques MultiPath, ce sont les chemins locaux (sur le client cible) qui sont utilisés en premier, quel que soit l'ordre défini. Le fichier `libtab` est ignoré avec des dispositifs à multiples chemins d'accès.

Configuration de périphériques dans un environnement SAN

L'environnement SAN peut varier d'un client utilisant une bibliothèque à plusieurs clients utilisant plusieurs bibliothèques. Les clients peuvent avoir différents systèmes d'exploitation. Du point de vue de Data Protector, la configuration d'un environnement SAN vise les objectifs suivants :

- Sur chaque hôte qui partagera le robot de la bibliothèque, créez une définition du robot de la bibliothèque pour chaque hôte. Si un seul hôte contrôle le robot, la définition de la bibliothèque est créée uniquement pour l'hôte de contrôle du robot par défaut.
- Sur chaque hôte qui participera au partage des mêmes lecteurs (bandes) de la bibliothèque :
  - Créez une définition de périphérique pour chaque périphérique à utiliser.
  - Utilisez un nom de verrouillage si le périphérique (physique) sera également utilisé par un autre hôte (périphérique partagé).
  - Vous pouvez également sélectionner un accès direct si vous souhaitez utiliser cette fonctionnalité. Si vous l'utilisez, vérifiez que le fichier `libtab` est configuré sur cet hôte.

Points à prendre en considération

- Microsoft Cluster Server : Assurez-vous que le chemin matériel du lecteur est le même sur les deux noeuds du cluster : une fois le périphérique configuré, effectuez un basculement afin de le vérifier.

Méthodes de configuration

Il existe trois méthodes de configuration qui dépendent des plates-formes participant à la configuration SAN :

Configuration automatique des périphériques en utilisant l'interface graphique

Vous pouvez utiliser la fonctionnalité de configuration automatique de Data Protector pour configurer automatiquement les périphériques et les bibliothèques sur plusieurs hôtes dans un environnement SAN. La configuration automatique est possible sur les systèmes d'exploitation suivants :

- Windows
- HP-UX
- Solaris

- Linux
- AIX

Limites

La configuration automatique ne peut pas être utilisée pour configurer les périphériques suivants dans un environnement SAN :

- bibliothèques de supports mixtes,
- bibliothèques DAS ou ACSLS,
- périphériques NDMP.

Data Protector découvre les périphériques de sauvegarde connectés à votre environnement. Pour les périphériques de bibliothèque, Data Protector détermine le nombre d'emplacements, le type de support et les lecteurs qui appartiennent à la bibliothèque. Data Protector configure ensuite le périphérique en définissant un nom logique, un nom de verrouillage, le type de support et l'adresse du fichier ou l'adresse SCSI du périphérique, ainsi que le lecteur et les emplacements.

> **REMARQUE :**
> Lorsque vous ajoutez un hôte dans un environnement SAN, les bibliothèques et les périphériques configurés ne sont pas mis à jour automatiquement.
>
> - Pour utiliser une bibliothèque existante sur un nouvel hôte, supprimez celle-ci et configurez-en automatiquement une nouvelle avec le même nom sur le nouvel hôte.
> - Pour ajouter des périphériques à une bibliothèque existante, vous pouvez supprimer la bibliothèque puis en configurer automatiquement une nouvelle avec le même nom et les nouveaux lecteurs sur un nouvel hôte ou ajouter manuellement les lecteurs à la bibliothèque.

Configuration automatique des périphériques en utilisant l'interface de ligne de commande (commande sanconf)

Vous pouvez configurer les périphériques et les bibliothèques d'un environnement SAN à l'aide de la commande `sanconf`. La commande `sanconf` est un utilitaire qui facilite la configuration des bibliothèques d'environnements SAN dans des cellules Data Protector uniques ainsi que dans des environnements MoM avec une base de données centralisée de gestion des supports (Centralized Media Management Database ou CMMDB). Elle peut configurer automatiquement une bibliothèque d'un environnement SAN en recueillant des informations sur les lecteurs de plusieurs clients puis en configurant ces clients dans une seule bibliothèque. Dans des environnements MoM, `sanconf` permet également de configurer toute bibliothèque d'une cellule Data Protector qui utilise CMMDB, à condition que la cellule dans laquelle `sanconf` est exécutée exécute également CMMDB. `sanconf` est disponible sur les systèmes d'exploitation suivants :

- Windows
- HP-UX
- Solaris

`sanconf` peut détecter et configurer les périphériques pris en charge et connectés à des clients exécutés sur les systèmes d'exploitation suivants :

- Windows
- HP-UX
- Solaris
- Linux
- AIX

Avec cette commande, vous pouvez :

- Analyser le système Data Protector spécifié afin de recueillir des informations sur les adresses SCSI des lecteurs et des contrôles de robots connectés aux clients dans l'environnement SAN.
- Configurer ou modifier les paramètres d'une bibliothèque ou d'un lecteyr pour des clients donnés en utilisant les informations recueillies lors de l'analyse des clients Data Protector.
- Supprimer les lecteurs de tous les clients ou de clients spécifiés d'une bibliothèque.

Verrouillage de périphérique

La commande `sanconf` crée automatiquement des noms de verrouillage pour les lecteurs qu'elle configure. Un nom verrouillage se compose de la chaîne ID fournisseur, de la chaîne ID produit et du numéro de série du produit.

Par exemple, le nom de verrouillage du lecteur HPE DLT 8000 avec l'ID fournisseur "HP", l'ID produit "DLT8000" et le numéro de série "A1B2C3D4E5" sera HP:DLT8000:A1B2C3D4E5.

Les noms de verrouillage peuvent également être ajoutés manuellement. Les noms de verrouillage sont uniques à chaque périphérique logique.

Vous ne devez pas modifier les noms de verrouillage qui ont été créés par la commande `sanconf`. Tous les autres lecteurs logiques créés manuellement et qui représentent des lecteurs physiques configurés par `sanconf` doivent également utiliser des noms de verrouillage créés par `sanconf`.

Limites

- Pour obtenir une liste complète des bibliothèques prises en charge par la commande `sanconf`, consultez les dernières matrices de support à l'adresse .https://softwaresupport.hpe.com/
- `sanconf` n'offre pas les fonctionnalités suivantes :
  - Installation de lecteurs de rechange dans les emplacements des lecteurs.
  - Combinaison de différents types de lecteurs ; par exemple, des combinaisons de lecteurs DLT, 9840 et LTO.
  - Configuration de clients actuellement indisponibles. La configuration de tels clients n'est possible que si la configuration de la bibliothèque est effectuée à l'aide d'un fichier de configuration contenant les informations recueillies après analyse des clients.

Recommandation

Configurez un seul pilote pour un périphérique spécifique sur un système.

Pour plus d'informations sur l'utilisation de la commande `sanconf`, reportez-vous à la page de manuel `sanconf` ou à la *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Configuration manuelle sur des systèmes UNIX

Lorsque vous configurez manuellement des périphériques partagés connectés aux systèmes UNIX d'un environnement SAN, vous devez:

- Créez une définition de périphérique pour chaque périphérique à utiliser.
- Utiliser un nom de verrouillage.
- Vous pouvez également sélectionner un accès direct si vous souhaitez utiliser cette fonctionnalité. Dans ce cas, vous devez vérifier que le fichier `libtab`sur cet hôte est correctement configuré.

Phases

1. Configurer manuellement les périphériques
2. Configurer manuellement le fichier libtab

À propos de la sauvegarde sur disque

La sauvegarde sur disque Data Protector enregistre les données sur des disques plutôt que sur une bande. Data Protector écrit sur des répertoires résidant sur un ou plusieurs disques. Les données sont enregistrées dans des fichiers stockés dans des répertoires du disque.

La sauvegarde sur disque est plus rapide que la sauvegarde sur bande car aucun processus mécanique, tel que le chargement de la bande, ne doit être déclenché avant l'exécution de la sauvegarde. Par ailleurs, le stockage sur disque devient de moins en moins onéreux.

La plupart des applications qui traitent des données stratégiques nécessitent la sauvegarde immédiate de chaque transaction qui vient d'être effectuée. La sauvegarde sur disque implique l'écriture permanente des données sur le disque tout au long de la journée.

Qu'est-ce qu'un périphérique de sauvegarde sur disque ?

Un périphérique de sauvegarde sur disque s'assimile à un lecteur de bande ou à un chargeur de bandes. Il comprend un ou plusieurs répertoires qui sont l'équivalent d'un référentiel dans un lecteur de bande. Lors d'une sauvegarde, le périphérique de sauvegarde sur disque écrit les données dans des dépôts de fichier de la même manière que des fichiers sur une bande. Étant donné qu'il écrit des données dans des fichiers résidant sur le disque, ce type de périphérique est également appelé "périphérique de fichier".

Configuration de périphériques de sauvegarde sur disque

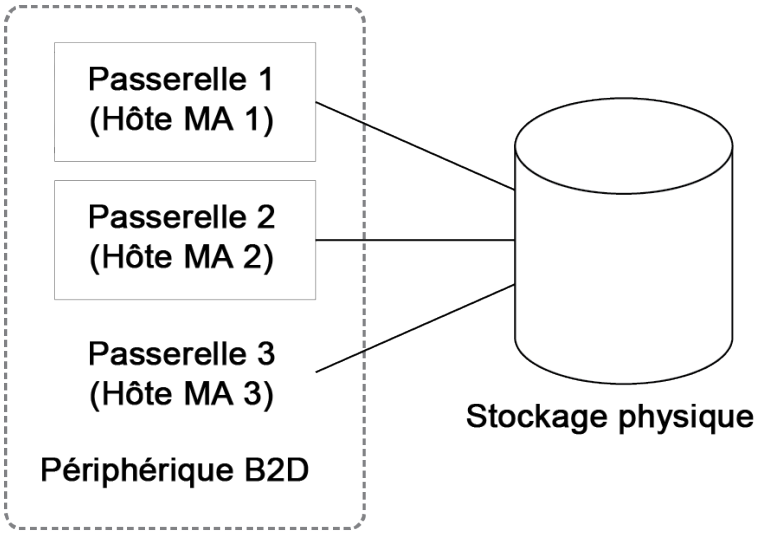
La configuration des périphériques de sauvegarde sur disque s'effectue par le biais de l'interface utilisateur graphique de Data Protector. Ceux-ci utilisent l'ensemble des fonctionnalités de gestion des supports, de sauvegarde et de restauration de Data Protector.

A propos des périphériques de sauvegarde sur disque

Un périphérique de sauvegarde sur disque (B2D) est un périphérique qui sauvegarde les données vers un stockage sur disque physique. Le périphérique B2D prend en charge les configurations multi-hôte. Cela signifie que plusieurs hôtes (passerelles) peuvent accéder à un même stockage. Chaque passerelle représente un client Data Protector sur lequel le composant Agent de support est installé. Le stockage physique peut également être partitionné en banques individuelles représentant des sections de stockage spécifiques (comme le partitionnement d'un disque dur). Chaque banque individuelle sur le stockage physique n'est accessible qu'à un seul périphérique B2D. Cependant, plusieurs périphériques B2D peuvent accéder à différentes banques sur le même stockage physique.

Bien que similaires à d'autres périphériques à base de bibliothèque, les périphériques B2D se comportent différemment car les passerelles offrent plus de flexibilité. Contrairement aux de lecteurs bibliothèque, chaque passerelle représente un hôte sur lequel plusieurs Agents de support peuvent être lancés simultanément, en sessions simples ou multiples.

Périphérique B2D (vue logique)



Le nombre d'Agents de support pouvant être démarrés sur une passerelle spécifique est défini par les éléments suivants :

- Les limites de la passerelle. Chaque passerelle B2D est limitée à un nombre maximal de flux parallèles.
- Limites de connexion de la banque. Cette limite est spécifiée dans l'interface graphique lors de la configuration d'un périphérique B2D. Si la valeur est laissée désactivée, Data Protector utilise la valeur maximale disponible.
- Les limites de connexion physiques de l'unité de stockage physique. Cette valeur est extraite de la mémoire physique.
- Selon l'opération en cours, chaque Gestionnaire de session tente d'équilibrer le nombre d'Agents de support sur une passerelle en tenant compte des paramètres d'entrée suivants :
  - Le nombre d'objets en cours de sauvegarde

- L'emplacement des objets
- Les restrictions physiques de connexion.

Les périphériques B2D utilisent un format de données spécial pour l'accès rapide en lecture/écriture, ce qui est incompatible avec le format de bande Data Protector standard. Le format de données est automatiquement défini lorsque vous sélectionnez un périphérique B2D.

À propos de la déduplication

La déduplication des données est une technologie de compression de données qui réduit la taille des données sauvegardées en ne sauvegardant pas les données dupliquées. Le processus de déduplication sépare les flux de données en morceaux (ou blocs) de données gérables. Les contenus de ces blocs de données sont ensuite comparés les uns aux autres. Si des blocs identiques sont détectés, ils sont remplacés par un pointeur vers un bloc unique. En d'autres termes, si 20 blocs identiques sont trouvés, un seul bloc est conservé (et sauvegardé) et les 19 autres sont remplacés par des pointeurs. Les données sauvegardées sont écrites sur un périphérique de destination sur disque appelé banque de déduplication. Lorsqu'une opération de restauration est terminée, le bloc unique est dupliqué puis inséré en bonne position comme identifié par le pointeur. Avec les opérations de restauration de type déduplication, le processus de restauration est parfois appelé réhydratation des données sauvegardées.

Quand effectuer une déduplication ?

Généralement, vous utilisez la déduplication de données pour sauvegarder un système d'e-mail pouvant contenir 100 instances d'une même pièce jointe contenant un fichier graphique de 1 Mo. Si le système est sauvegardé en utilisant une technique de sauvegarde standard, les 100 instances de pièces jointes sont toutes sauvegardées. Cela nécessite environ 100 Mo d'espace de stockage. Cependant, avec la déduplication des données, une seule instance de la pièce jointe est réellement stockée. Toutes les autres instances font référence à la copie stockée unique. Dans cet exemple, le *taux de déduplication* est de 100 pour 1 environ. Bien que cet exemple illustre une déduplication au niveau des fichiers, il sert à démontrer les avantages de l'utilisation de périphériques de sauvegarde sur disque et de la déduplication.

Avantages de la déduplication

En règle générale, la déduplication des données augmente la vitesse du service de sauvegarde dans son ensemble et réduit le coût global du stockage. La déduplication des données réduit considérablement l'espace de stockage sur disque requis. Comme la déduplication des données est un système basé sur disque, les niveaux du service de restauration sont nettement plus élevés et les erreurs de gestion de bande (ou autre support) sont moindres.

Technologies de déduplication

Il existe plusieurs technologies de déduplication disponibles sur le marché. Elles sont généralement regroupées en solutions matérielles et logicielles. Ces solutions peuvent être subdivisées, par exemple, au niveau des fichiers (instanciation unique) ou au niveau des blocs.

Data Protector prend en charge les solutions de déduplication suivantes :

Déduplication logicielle StoreOnce

La déduplication logicielle StoreOnce de Data Protector offre une solution logicielle de déduplication au niveau des blocs.

Lorsque vous utilisez la déduplication logicielle StoreOnce, tenez compte des éléments suivants :

- La déduplication sauvegarde uniquement les périphériques sur disque. Elle ne peut pas être utilisée avec des supports amovibles tels que des lecteurs de bande ou des bibliothèques.
- Comme Data Protector utilise uniquement une approche logicielle pour la déduplication (lors de la déduplication logicielle StoreOnce), aucun matériel spécifique n'est requis autre que des disques durs standard pour stocker les données sauvegardées.
- La déduplication logicielle StoreOnce utilise une technologie de segmentation par hachage pour séparer le flux de données en gros blocs de données.
- Lors du processus de déduplication, les données dupliquées sont supprimées, ne laissant qu'une seule copie des données à stocker, ainsi que des liens de référence vers l'unique exemplaire. La déduplication permet de réduire la capacité de stockage requise puisque seules les données uniques sont stockées.
- Spécifier un périphérique cible de sauvegarde sur disque dans la spécification de sauvegarde indique à Data Protector d'effectuer une sauvegarde de type déduplication.

Périphériques du système de sauvegarde HPE StoreOnce

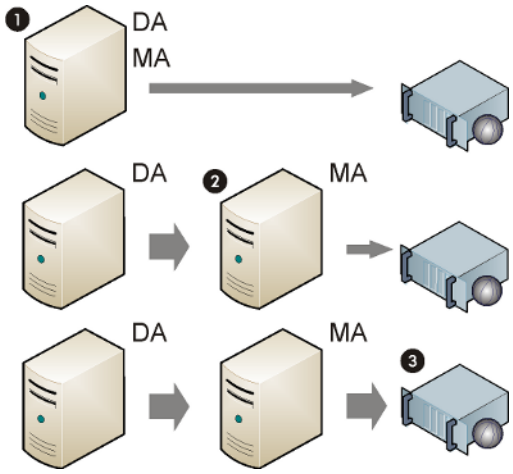
Les périphériques du système de sauvegarde HPE StoreOnce sont des périphériques de sauvegarde disque à disque (D2D) prenant en charge la déduplication.

Configuration de la déduplication

Data Protector prend en charge différentes configurations de déduplication :

- Déduplication côté source (1) —les les données sont dédupliquées à la source (le système sauvegardé).
- Déduplication côté serveur (2) —les données sont dédupliquées sur le système Agent de support (la passerelle).
- Déduplication côté cible (3) — les données sont dédupliquées sur le périphérique cible (système de sauvegarde StoreOne ou système logiciel StoreOnce).

Configurations de déduplication



Déduplication côté source

Dans une déduplication côté source (1), un Agent de support est installé avec l'Agent de disque sur le client sauvegardé, et le client devient donc une passerelle (passerelle côté source). La déduplication est réalisée par l'Agent de support sur le client lui-même afin que les données dédupliquées soient envoyées au périphérique cible, réduisant ainsi le trafic réseau global. Le nombre de flux simultanés est limité par les paramètres de partage de charge. Lorsqu'un Agent de support termine la sauvegarde d'objets locaux, un nouvel Agent de support est démarré sur le prochain système client. Notez que le système sauvegardé doit prendre en charge la déduplication.

Déduplication côté serveur

Dans une déduplication côté serveur, la déduplication est effectuée sur un client Agent de support distinct (passerelle) par l'Agent de support. Cela réduit la charge sur le système sauvegardé et sur le périphérique cible, mais sans diminuer le volume de trafic réseau entre l'Agent de disque et l'Agent de support.

Notez que le client Agent de support doit prendre en charge la déduplication. La déduplication côté serveur vous permet de dédupliquer les données de clients pour lesquels la déduplication n'est pas prise en charge localement.

Déduplication côté cible

Le processus de déduplication a lieu sur le périphérique cible. Il reçoit les données à sauvegarder des Agents de support installés sur les clients (passerelles). La déduplication côté cible ne réduit pas le volume de trafic réseau entre l'Agent de support et le système de déduplication.

À propos des périphériques de bibliothèque de fichiers

Un périphérique de bibliothèque de fichiers est un périphérique qui réside dans un répertoire sur un disque dur interne ou externe que vous avez défini. Un périphérique de bibliothèque de fichiers comprend un ensemble de répertoires. Lorsqu'une sauvegarde est effectuée sur le périphérique, des fichiers sont automatiquement créés dans ces répertoires. Les fichiers contenus dans les répertoires de la bibliothèque de fichiers sont appelés dépôts de fichier.

Data Protector ne fixe aucune limite de capacité maximale pour les périphériques de ce type. La seule limite de taille est constituée par la taille maximale du système de fichiers sur lequel réside le répertoire. Par exemple, la taille maximale du périphérique de bibliothèque de fichiers sous Linux correspond à la taille maximale des fichiers que vous pouvez enregistrer sous ce système d'exploitation.

Vous indiquez la capacité de chaque dépôt de fichier dans le périphérique de bibliothèque de fichiers lors de la configuration initiale de ce dernier. Vous pouvez redéfinir les propriétés de taille des dépôts de fichier à tout moment lors de l'utilisation du périphérique, au moyen des propriétés de la bibliothèque de fichiers.

Le périphérique de bibliothèque de fichiers peut être situé sur un disque dur local ou externe, à condition que Data Protector connaisse son chemin d'accès. Précisez le chemin d'accès lorsque vous configurez le périphérique.

Gestion des périphériques de sauvegarde sur disque

Si le périphérique de sauvegarde sur disque que vous utilisez est plein, vous devez effectuer l'une des opérations suivantes avant de continuer à réaliser des sauvegardes avec celui-ci :

- Commencer à déplacer des données sur bande pour libérer le périphérique ou un ou plusieurs emplacements de fichiers.
- Recycler les dépôts de fichier.
- Ajouter un nouveau dépôt de fichier au périphérique.

Dépôts de fichier

Les dépôts de fichier sont les fichiers contenant les données d'une sauvegarde vers un périphérique de bibliothèque de fichiers.

Création des dépôts de fichier

Lors du lancement de la première sauvegarde à l'aide du périphérique de bibliothèque de fichiers, Data Protector crée automatiquement des dépôts de fichier dans le périphérique. Data Protector crée un dépôt de fichier pour chaque session de sauvegarde de données effectuée en utilisant le périphérique. Si la quantité de données à sauvegarder est supérieure à la taille maximale par défaut d'un dépôt de fichier, Data Protector crée plusieurs dépôts de fichier pour une session de sauvegarde.

Nom de dépôt de fichier

Le nom de chaque dépôt de fichier est un identificateur unique attribué automatiquement par le système.

Data Protector ajoute également un identificateur de support au dépôt de fichier. Il identifie le dépôt de fichier en tant que support dans le pool de supports. L'identificateur ajouté au support permet d'identifier une session de sauvegarde particulière lors d'une restauration. L'identificateur est indiqué lors de l'affichage des propriétés du dépôt de fichier.

Notez que si le dépôt de fichier a été recyclé, son nom peut disparaître de l'interface bien que son icône continue à y figurer.

Taille de dépôt de fichier

La taille des dépôts de fichier est définie lors de la création initiale du périphérique de bibliothèque de fichiers. Vous spécifiez alors toutes les propriétés de taille du périphérique, notamment la taille maximale des dépôts de fichier. Les propriétés de taille des dépôts de fichier ne sont définies qu'une seule fois, mais appliquées globalement à chaque dépôt de fichier. Si la quantité de données à sauvegarder dans une session est supérieure à la taille de dépôt de fichier initialement spécifiée, Data Protector crée automatiquement d'autres dépôts de fichier jusqu'à ce que l'espace disque alloué au périphérique soit occupé.

La taille par défaut du dépôt est de 5 Go. Vous pouvez augmenter cette valeur (jusqu'à 2 To), mais au risque de dégradations des performances.

Espace utilisé par les dépôts de fichier

Data Protector crée automatiquement des dépôts de fichier jusqu'à ce que le périphérique ne possède plus d'espace disque disponible. La quantité d'espace qui doit rester libre pour le périphérique de bibliothèque de fichiers est définie dans les propriétés du périphérique lors de sa configuration initiale.

Gestion des disques pleins

Si l'espace disque total disponible sur le périphérique de bibliothèque de fichiers devient inférieur à un niveau spécifié, une notification est émise.

Nombre de périphériques par disque

Le périphérique de bibliothèque de fichiers peut inclure un ou plusieurs répertoires. Un seul répertoire peut se trouver dans un système de fichiers.

Au cas où les dépôts de fichier se trouvent sur plusieurs disques, il est déconseillé de placer sur un même disque les dépôts de fichier de deux périphériques différents. En effet, si les propriétés sont différentes, un conflit peut se produire dans Data Protector (par exemple, si l'espace disque restant spécifié pour le dépôt de fichier est de 20 Mo sur un périphérique de bibliothèque de fichiers et de 10 Mo sur l'autre).

Définition des propriétés d'un périphérique de bibliothèque de fichiers

Les propriétés d'un périphérique de bibliothèque de fichiers peuvent être définies au cours de la configuration initiale de ce périphérique ou être modifiées une fois que le périphérique est opérationnel.

Configuration initiale des propriétés

Procédure

1. Lors de la configuration du périphérique de bibliothèque de fichiers, sélectionnez le répertoire du périphérique, puis cliquez sur **Propriétés**.

2. Spécifiez les propriétés de taille du périphérique. Cliquez sur **OK**.
3. Cliquez sur **Suivant** et poursuivez la configuration du périphérique de bibliothèque de fichiers.

Modification des propriétés d'un périphérique

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Périphériques**, puis cliquez sur le nom du périphérique de bibliothèque de fichiers à modifier.
3. Cliquez avec le bouton droit sur le nom du périphérique de bibliothèque, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Référentiel**. Dans la liste, sélectionnez le chemin d'accès à la bibliothèque de fichiers.
5. Cliquez sur les **Propriétés**. Spécifiez toutes les propriétés de taille du périphérique, puis cliquez sur **OK**.

Data Protector applique ensuite les nouvelles propriétés spécifiées à chaque dépôt de fichier créé sur le périphérique de bibliothèque de fichiers. Les propriétés des dépôts de fichier créés avant la modification des propriétés du périphérique ne sont pas affectées.

Suppression de périphériques de bibliothèque de fichiers

Pour supprimer un périphérique de bibliothèque de fichiers, vous devez vous assurer qu'il ne contient aucune donnée protégée. Cela signifie qu'avant de pouvoir supprimer la bibliothèque de fichiers, vous devez modifier le niveau de protection des données sur chaque dépôt de fichier contenu dans le périphérique.

Phases de suppression

1. Vérification de la protection des données
2. Recyclage des dépôts de fichier
3. Suppression de l'icône du dépôt de fichier exporté
4. Suppression du périphérique de bibliothèque de fichiers

Vérification de la protection des données

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, sélectionnez le nom du périphérique de bibliothèque de fichiers à supprimer et ouvrez le dossier Répertoires dans la bibliothèque de fichiers.
3. La zone de résultats, localisez la colonne Protection Recherchez les dépôts de fichier ayant un niveau de protection Permanent.

Recyclage des dépôts de fichier

Vous pouvez libérer de l'espace disque en recyclant et supprimant des dépôts de fichier ou des périphériques de bibliothèque de fichiers entiers.

Vous pouvez recycler certains dépôts de fichier ou tous ceux d'une bibliothèque de fichiers. Ceci permet de récupérer et d'utiliser pour la prochaine sauvegarde l'espace disque occupé par l'élément recyclé. Pour ce faire, supprimez les dépôts de fichier non protégés et créez-en de nouveaux.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez les dépôts de fichier du périphérique de bibliothèque de fichiers.
3. Dans la zone de résultats, sélectionnez les dépôts de fichier à recycler en cliquant sur leur nom.
4. Cliquez avec le bouton droit sur le dépôt sélectionné, puis cliquez sur **Exporter**.

   L'exportation d'un dépôt de fichier supprime les informations sur celui-ci dans la base de données interne (IDB). Data Protector cesse alors de considérer que le dépôt de fichier existe. Toutefois, les informations sont néanmoins conservées, et vous pouvez les importer ultérieurement si vous avez besoin de récupérer le dépôt de fichier.
5. Cliquez avec le bouton droit sur le dépôt sélectionné, puis cliquez sur **Recycler**.
6. Répétez cette opération pour chaque dépôt de fichier de la bibliothèque de fichiers ayant un niveau de protection de données complet.

Une fois que vous avez marqué un dépôt de fichier pour le recyclage, le nom correspondant qui est automatiquement généré par Data Protector disparaît et seule l'icône du dépôt est visible dans l'interface utilisateur graphique de Data Protector. Il est possible de supprimer l'icône du dépôt de fichier exporté.

Suppression de l'icône du dépôt de fichier exporté

Une fois un dépôt de fichier exporté, son nom disparaît, et seule son icône est visible dans le Gestionnaire Data Protector.

Procédure

1. Dans la zone de résultats, sélectionnez l'icône à supprimer.
2. Cliquez avec le bouton droit sur l'icône sélectionnée, puis cliquez sur **Supprimer**.
3. Répétez cette opération pour chaque icône de dépôt de fichier exporté à supprimer.

Vous supprimez ainsi l'icône de l'interface, mais pas le fichier résidant dans la base de données interne.

Suppression du périphérique de bibliothèque de fichiers

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, sélectionnez le nom du périphérique de bibliothèque de fichiers à supprimer.
3. Cliquez avec le bouton droit sur le périphérique, puis cliquez sur **Supprimer**.

Le périphérique de bibliothèque de fichiers est alors supprimé de la base de données interne.

A propos des périphériques de bibliothèque de stockage

Périphériques physiques de bibliothèque de stockage

Une bibliothèque de bandes magnéto-optiques est un périphérique de bibliothèque qui peut contenir des supports optiques ou des fichiers. Si les supports sont des fichiers, elle est appelée "périphérique de bibliothèque de stockage de fichiers". Le type de support sur le périphérique est défini lors de la configuration initiale. Si vous utilisez une bibliothèque de bandes-optique sous UNIX, vous devez configurer un fichier de périphérique UNIX pour chaque emplacement de l'échangeur ou face du disque.

Périphériques de fichier de bibliothèque de stockage

Ce type de périphérique est un équivalent logique d'un chargeur de bandes. Il contient des emplacements dont la taille est définie par l'utilisateur lors de la configuration initiale du périphérique. Ce périphérique est configuré manuellement. Ses propriétés sont modifiables pendant son utilisation. Si les supports utilisés sont des fichiers, le périphérique écrit les données sur le disque et non sur une bande. Le périphérique de bibliothèque de stockage de fichiers enregistre les données sous forme de fichiers. Chacun de ces fichiers est l'équivalent d'un emplacement dans un périphérique à bandes.

La capacité maximale de stockage recommandée de ce périphérique n'est limitée que par la quantité de données que peut stocker le système d'exploitation utilisé dans un système de fichiers. Chaque emplacement du périphérique de bibliothèque de stockage de fichiers a une capacité maximale de 2 To. Toutefois, il est normalement recommandé de conserver une taille d'emplacement comprise entre 100 Mo et 50 Go (sur des systèmes Windows), ou entre 100 Mo et 2 To (sur des systèmes UNIX). Si, par exemple, vous devez sauvegarder 1 To de données, vous pouvez utiliser la configuration de périphérique suivante :

Systèmes Windows : Un périphérique de bibliothèque de stockage de fichiers avec 100 emplacements de fichiers de 10 Go chacun

Systèmes UNIX : Un périphérique de bibliothèque de stockage de fichiers avec 250 emplacements de fichiers de 4 Go chacun

Pour améliorer les performances du périphérique, il est recommandé de n'utiliser qu'un périphérique par disque et un lecteur par périphérique. En outre, il faut éviter que d'autres applications ne transfèrent de grandes quantités de données vers/à partir du disque lors de l'exécution d'une sauvegarde ou restauration Data Protector.

Tailles d'emplacement recommandées pour Windows et UNIX

Espace disque disponible	Nombre d'emplacements	Taille d'emplacement
1 To	100	10
5 TB	250	20
10 TB	250	40

Gestion des périphériques de bibliothèque de stockage de fichiers

Si le périphérique de bibliothèque de stockage de fichiers que vous utilisez est plein, vous devez effectuer l'une des opérations suivantes avant de continuer à réaliser des sauvegardes avec celui-ci :

- Commencer à déplacer des données sur bande pour libérer le périphérique ou un ou plusieurs emplacements de fichiers.
- Recycler un ou des emplacements du périphérique.
- Ajouter un nouvel emplacement au périphérique.

Configuration d'un périphérique de bibliothèque de stockage de fichiers

Il est recommandé que le périphérique que vous créez se trouve sur un disque autre que celui contenant l'IDB. Ceci garantit la disponibilité d'une quantité d'espace disque suffisante pour la base de données. En outre, le placement du périphérique et de l'IDN sur des disques distincts améliore les performances.

Configuration d'un périphérique de bibliothèque de stockage de fichiers

> **IMPORTANT :**
> Prenez en compte ce qui suit :
>
> - N'utilisez pas le nom d'un périphérique existant pour configurer celui-ci, car il serait alors écrasé.
> - N'utilisez pas le même nom pour configurer plusieurs périphériques, car il serait alors écrasé lors de chaque accès au périphérique.

Conditions préalables

- Sur les systèmes Windows, désactivez l'option de compression Windows pour le fichier que vous voulez utiliser comme périphérique.
- Vous devez créer sur le disque le répertoire dans lequel résidera le périphérique avant de créer ce dernier.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
3. Dans la zone de texte Nom de périphérique, saisissez le nom du périphérique.
4. Dans la zone de texte Description, vous pouvez saisir une description (facultatif).
5. Dans la liste Type de périphérique, sélectionnez **Bibliothèque de bandes magnéto-optiques**.
6. Dans la liste Client, sélectionnez le nom du client.
7. Dans la zone de texte relative à l'adresse URL de la console de gestion, entrez une URL valide pour la console de gestion de bibliothèque (facultatif).
8. Cliquez sur **Suivant**.
9. Indiquez un ensemble de fichiers/disques pour la bibliothèque de bandes magnéto-optiques. Utilisez un tiret pour spécifier plusieurs fichiers ou disques à la fois (`/tmp/FILE 1-3`, par exemple), puis cliquez sur **Ajouter**. Pour les bibliothèques de bandes magnéto-optiques, les noms de disque doivent se terminer par `A/a` ou `B/b`. Cliquez sur **Suivant**.
10. Dans la liste Type de support, sélectionnez **Fichier** pour le périphérique que vous êtes en train de configurer.
11. Cliquez sur **Terminer** pour quitter cet assistant. Il vous est alors demandé de configurer un lecteur de bibliothèque. Cliquez sur **Oui** pour afficher l'assistant de configuration.

Configuration d'un lecteur dans le périphérique de bibliothèque de stockage de fichiers

Procédure

1. Dans la zone de texte Nom de périphérique, saisissez le nom du périphérique.
2. Dans la zone de texte Description, vous pouvez éventuellement saisir une description.
3. Indiquez un pool de supports pour le type de support sélectionné. Vous pouvez soit sélectionner un pool dans la liste Pool de supports, soit saisir un nouveau nom de pool. Dans ce cas, le pool sera créé automatiquement. Vous pouvez configurer un pool de supports pour tous les lecteurs ou choisir un pool de supports indépendant pour chaque lecteur. Cliquez sur **Suivant**.
4. Le cas échéant, vous pouvez aussi sélectionner **Le périphérique peut être utilisé pour la restauration** et/ou **Le périphérique peut être utilisé comme source pour la copie d'objets** et indiquer une **balise de périphérique**.
5. Cliquez sur **Terminer** pour quitter l'assistant.

Le nom du lecteur s'affiche dans la liste des lecteurs configurés. Vous pouvez analyser les lecteurs pour en vérifier la configuration.

Recyclage d'un emplacement de bibliothèque de stockage de fichiers

La protection des données est définie pour chaque emplacement de fichier dans une bibliothèque de stockage, ce qui permet de recycler un seul emplacement en mettant sa Protection sur **Aucun**e. La disponibilité de plusieurs petits emplacements peut ainsi améliorer la flexibilité et l'efficacité de la protection des données et de la gestion de l'espace libre. Le recyclage d'un emplacement de périphérique de bibliothèque de stockage de fichiers entraîne l'annulation de la protection des données ; de cette manière, cet emplacement puisse être réutilisé pour la sauvegarde. Les données de l'emplacement seront écrasées au cours de la prochaine session de sauvegarde.

> **IMPORTANT :**
> En cas d'emploi de cette méthode, les données existantes du support sont écrasées et perdues.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez les emplacements du périphérique de bibliothèque de stockage de fichiers.
3. Dans la zone de résultats, sélectionnez les emplacements à recycler.
4. Cliquez avec le bouton droit sur l'emplacement sélectionné et cliquez sur Recycler.

A propos des périphériques autonomes

Périphériques physiques autonomes

Un périphérique autonome est un simple périphérique comportant un lecteur qui lit ou écrit sur un support à la fois, DDS ou DLT par exemple. Ces périphériques sont utilisés pour les sauvegardes à petite échelle. Dès que le support est plein, un opérateur doit le remplacer manuellement par un nouveau support afin de poursuivre la sauvegarde. Les périphériques autonomes ne conviennent donc pas pour les grandes sauvegardes sans surveillance.

Périphériques de fichier autonomes

Un périphérique de fichier autonome est un fichier résidant dans un répertoire déterminé, dans lequel vous sauvegardez des données au lieu de les écrire sur une bande. Il enregistre les données sous forme de fichiers. Chacun de ces fichiers est l'équivalent d'un emplacement dans un périphérique à bandes. Le périphérique de fichier autonome est utile pour réaliser des sauvegardes moins importantes.

La capacité maximale d'un périphérique de fichier est de 2 To. Toutefois, il est normalement recommandé de conserver une taille de périphérique comprise entre 100 Mo et 50 Go sur des systèmes Windows, ou entre 100 Mo et 2 To sur des systèmes UNIX. Data Protector ne mesure jamais l'espace disque libre dans le système de fichiers. Il considère la capacité par défaut ou la capacité spécifiée comme la taille limite de fichier. Vous ne pouvez pas utiliser de fichiers compressés pour ce type de

périphérique. Vous pouvez modifier la taille de fichier par défaut en définissant l'option globale `FileMediumCapacity`.

La taille maximale par défaut d'un périphérique de fichier autonome est de 100 Mo. Si vous souhaitez effectuer une sauvegarde plus volumineuse, modifiez la taille de fichier par défaut en définissant l'option globale `FileMediumCapacity`. Pour plus d'informations sur la définition des options globales, voir Personnalisation des options globales de HPE Data Protector ou Personnalisation d'options en éditant le fichier global.

Par exemple, pour une taille maximale de 20 Go (20 Go = 20 000 Mo), définissez ainsi l'option globale `FileMediumCapacity` :

```
# FileMediumCapacity=MaxSizeInMBytes

FileMediumCapacity=20000
```

Vous indiquez la capacité d'un périphérique de fichiers lorsque vous formatez le support. Si vous reformatez le support et spécifiez une nouvelle taille, c'est la taille initiale qui est utilisée. Vous pouvez changer la capacité d'un périphérique de fichier uniquement en supprimant le fichier du système.

La taille spécifiée doit être d'au moins 1 Mo inférieure à l'espace maximum libre sur le système de fichiers. Lorsqu'un périphérique de fichier atteint sa taille limite, Data Protector émet une demande de montage.

Pour améliorer les performances du périphérique, il est recommandé de n'utiliser qu'un périphérique par disque et un lecteur par périphérique. En outre, il faut éviter que d'autres applications ne transfèrent de grandes quantités de données vers/à partir du disque lors de l'exécution d'une sauvegarde ou restauration Data Protector.

Le fichier peut être situé sur un disque dur local ou externe, à condition que Data Protector connaisse son chemin d'accès. Précisez le chemin d'accès lorsque vous configurez le périphérique de fichier.

Configuration d'un périphérique de fichier autonome

Il est recommandé que le périphérique que vous créez se trouve sur un disque autre que celui contenant l'IDB. Ceci garantit la disponibilité d'une quantité d'espace disque suffisante pour la base de données. En outre, le placement du périphérique et de l'IDN sur des disques distincts améliore les performances.

> **IMPORTANT :**
> Prenez en compte ce qui suit :
>
> - N'utilisez pas le nom d'un périphérique existant pour configurer celui-ci, car il serait alors écrasé.
> - N'utilisez pas le même nom pour configurer plusieurs périphériques, car il serait alors écrasé lors de chaque accès au périphérique.

Conditions préalables

- Sur les systèmes Windows, désactivez l'option de compression Windows pour le fichier que vous voulez utiliser comme périphérique.
- Vous devez créer sur le disque le répertoire dans lequel résidera le périphérique avant de créer ce dernier.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Périphériques**, puis cliquez sur **Ajouter périphérique** pour ouvrir l'assistant.
3. Dans la zone de texte Nom du périphérique, entrez un nom pour le périphérique.
4. Dans la zone de texte Description, vous pouvez saisir une description (facultatif).
5. Dans la liste Client, sélectionnez le nom du client.
6. Dans la liste Type de périphérique, sélectionnez le type de périphérique **Autonome**, puis cliquez sur **Suivant**.
7. Dans la zone de texte, saisissez le chemin d'accès au périphérique de fichier, par exemple `c:\My_Backup\file_device.bin`.
8. Cliquez sur **Ajouter**, puis sur **Suivant**.
9. Dans la liste Type de support, sélectionnez un type de support **Fichier**.
10. Indiquez un pool de supports pour le type de support sélectionné. Vous pouvez soit sélectionner un pool dans la liste déroulante Pool de supports, soit saisir un nouveau nom de pool. Dans ce cas, le pool sera créé automatiquement.
11. Cliquez sur **Terminer** pour quitter l'assistant.

Le nom du périphérique s'affiche dans la liste de périphériques configurés. Vous pouvez analyser le périphérique pour en vérifier la configuration.

A ce stade, le périphérique a été spécifié pour Data Protector, mais il n'existe pas encore réellement sur disque. Avant de l'utiliser pour une sauvegarde, vous devez le formater.

Chapitre 9: Supports

À propos de la gestion de supports

Data Protector propose des fonctionnalités de gestion des supports très puissantes qui permettent de gérer simplement et efficacement un grand nombre de supports. Le système utilise l'IDB pour stocker les informations relatives aux sauvegardes, aux restaurations et à la gestion des supports.

Parmi les fonctions avancées de gestion des supports de Data Protector figurent les suivantes :

- La protection contre les écrasements accidentels.
- Pools de supports permettant de travailler sur de grands groupes de supports sans avoir à vous préoccuper de chaque support en particulier.
- La capacité de transférer l'ensemble des données de catalogue relatives aux supports d'un Gestionnaire de cellule Data Protector à un autre sans accéder physiquement aux supports.
- La fonctionnalité pool libre qui permet d'éviter l'échec d'une sauvegarde à cause d'un manque de supports libres.
- Le suivi de tous les supports et de l'état de chaque support, ainsi que le partage de ces informations entre plusieurs cellules Data Protector : délai d'expiration de la protection de données, disponibilité des supports pour les sauvegardes et un catalogue des données sauvegardées sur chaque support.
- La possibilité de définir explicitement les supports et les périphériques à utiliser pour une sauvegarde donnée.
- La reconnaissance automatique des supports Data Protector et autres formats de bandes courants.
- La reconnaissance et le support des codes-barres sur de grands périphériques de bibliothèque et périphériques silo disposant d'un support de code-barres.
- La centralisation des informations relatives aux supports, qui peuvent être partagées entre plusieurs cellules Data Protector.
- Prise en charge de la mise au coffre des supports. Cette opération est également connue sous le nom d'archivage ou de stockage hors site.
- La création interactive ou automatique de copies supplémentaires des données figurant sur le support.
- Paramètres de filtrage détaillé et de pagination.

Personnalisation de l'affichage des périphériques et des supports

Vous pouvez personnaliser la vue par défaut du contexte Périphériques et Supports en configurant les options globales `MediaView`, `MagazineView`, `SCSIView`, `ExternalView`, `JukeboxView`, `ACSView` et `DASView`. Personnalisez les attributs qui s'afficheront dans le contexte de bibliothèque ou de gestion de support en spécifiant les chaînes de jetons correspondantes. Pour plus d'informations, consultez Personnalisation des options globales de HPE Data Protector.

À propos des pools de supports

Un pool de supports est un jeu de supports du même type utilisé pour effectuer des sauvegardes. Vous pouvez posséder un pool de supports pour une sauvegarde normale, un pour une sauvegarde d'archives, un pour chaque service, etc. Chaque pool de supports est caractérisé par l'utilisation des supports, la stratégie d'allocation et les facteurs d'état de support.

Pools libres

Un pool libre est une source auxiliaire de supports du même type, disponibles lorsque tous les supports d'un pool sont utilisés. Les pools libres permettent d'éviter l'échec de sauvegardes dû à un manque de supports libres.

Les supports protégés appartiennent à un pool spécifique (à un pool SAP par exemple), alors que les supports libres peuvent être déplacés automatiquement vers un pool libre utilisé par plusieurs autres pools. Ce dernier sert ensuite à allouer des supports libres à tous les pools qui l'utilisent. Vous pouvez choisir d'associer ou non un pool libre à chacun des pools de supports.

Pool de supports par défaut

Un pool de supports par défaut est un pool fourni par Data Protector et qui fait partie de la définition d'un périphérique. Ce pool est utilisé si aucun autre n'est défini dans la spécification de sauvegarde.

Caractéristiques des pools libres

Un pool de supports est un pool de supports que vous pouvez configurer de façon à répartir les supports libres entre les pools de supports, ce qui permet de réduire les interventions de l'opérateur suite à des demandes de montage. L'utilisation d'un pool libre est facultative.

Un pool libre possède certaines caractéristiques qu'il est important d'examiner avant d'utiliser le pool.

Propriétés d'un pool libre

Un pool libre :

- ne peut pas être supprimé en cas de lien à un pool de supports ou s'il n'est pas vide.
- est différent d'un pool normal car, ne pouvant contenir des supports protégés, il ne peut pas être utilisé pour l'allocation. Les options de stratégie d'allocation (Stricte / Souple, Ajout possible / Sans possibilité d'ajout) ne sont donc pas disponibles.
- ne contient que des supports Data Protector libres (supports inconnus ou vierges exclus).

Quand utilise-t-on un pool libre ?

Un support est déplacé d'un pool normal vers un pool libre, et vice versa, dans deux cas :

- S'il n'y a aucun support libre dans le pool normal, Data Protector alloue les supports du pool libre. Le support est automatiquement déplacé vers le pool normal.

- Lorsque toutes les données qui se trouvent sur le support (situé dans un pool normal) expirent, le support peut être déplacé automatiquement vers le pool libre.

Calcul de la qualité des supports

La qualité des supports est déterminée sur une base d'égalité entre les pools "associés". Les Facteurs d'état des supports sont configurables pour un pool libre uniquement, et tous les pools utilisant le pool libre héritent de ses facteurs. Une base de détermination distincte est appliquée pour les pools n'utilisant pas le pool libre.

Limites des pools libres

- Vous ne pouvez pas déplacer un support protégé vers un pool libre.
- Vous ne pouvez pas effectuer certaines opérations sur un support, telles que l'importation, la copie et le recyclage, car elles sont susceptibles d'affecter un support protégé.
- Les pools pour lesquels l'option prise en charge de magasins est sélectionnée ne peuvent pas utiliser de pool libre.
- Certaines incohérences provisoires (une journée) peuvent apparaître dans des pools lorsque vous utilisez des pools libres (par exemple lorsqu'un support non protégé qui se trouve dans un pool normal est en attente de désallocation vers le pool libre).
- Si un pool libre contient des supports ayant différents types de formats de données, Data Protector reformate automatiquement les supports alloués, si nécessaire. Par exemple, un support NDMP peut être reformaté en support normal.

Propriétés des pools de supports

Vous spécifiez les attributs de pools de support lors de la configuration d'un pool de supports. Vous pourrez par la suite changer certaines propriétés.

Pour plus d'informations sur les propriétés des pools de supports, consultez Aide de HPE Data Protector.

Propriétés des pools de supports - Général

- Description
- Nom de pool
- Type de support

Propriétés des pools de supports - Allocation

Allocation

La stratégie d'allocation de support permet de définir l'ordre dans lequel les supports d'un pool doivent être utilisés, afin que leur usure soit uniforme. Les options relatives à cette stratégie sont les suivantes :

- Stratégie stricte
- Stratégie souple
- Allouer d'abord support non formaté
- Utiliser pool libre
- Déplacer support libre vers pool libre
- Support de magasin

Propriétés des pools de supports - Etat

Facteurs d'état des supports

Les facteurs d'état des supports permettent de déterminer leur état, et donc la durée pendant laquelle ils peuvent être utilisés de façon fiable pour la sauvegarde. Par exemple, une sauvegarde sur un support abîmé ou ancien risque plus de produire des erreurs de lecture ou d'écriture. En fonction de ces facteurs, Data Protector change l'état des supports, de bon à passable ou à médiocre. Les facteurs d'état sont définis pour l'ensemble du pool de supports, et non pour chaque support.

IMPORTANT :
Pour que Data Protector détermine exactement l'état des supports, utilisez de nouveaux supports en cas d'ajout au pool de supports.

REMARQUE :
Si un pool utilise l'option de pool libre, les facteurs d'état des supports sont hérités du pool libre.

Vous pouvez sélectionner les deux facteurs d'état de support suivants :

- Nombre maximum d'écrasements
- Valide pendant (mois)

Propriétés des pools de supports - Utilisation

Cette stratégie permet de déterminer les modalités d'ajout des nouvelles sauvegardes aux supports déjà utilisés. Les options relatives à cette stratégie sont les suivantes :

- Ajout possible
- Sans possibilité d'ajout
- Ajout possible aux incrémentales uniquement

Qualité des pools de supports

Le support ayant la plus mauvaise qualité dans un pool détermine la qualité du pool de support. Par exemple, dès que la qualité de l'un des supports du pool devient médiocre, tout le pool est marqué comme médiocre.

La qualité des supports est déterminante pour leur sélection dans le cadre d'une sauvegarde, car elle a une incidence sur la capacité à lire ou à écrire des données sur ceux-ci. Les supports en bon état sont

sélectionnés en priorité par rapport aux supports d'état passable. Les supports d'état médiocre ne sont pas sélectionnés pour la sauvegarde.

L'état des supports est déterminé par l'un des facteurs d'état suivants :

- En bon état
- Passable
- Médiocre

Vous pouvez modifier les facteurs d'état utilisés pour déterminer l'état d'un support dans la page de propriétés Etat des propriétés du pool de supports. Les nouveaux facteurs d'état des supports sont utilisés pour déterminer l'état de l'ensemble des supports du pool.

Erreur de périphérique et qualité des supports

Si une erreur se produit au niveau du périphérique pendant une sauvegarde, le support utilisé pour la sauvegarde avec ce périphérique se voit attribuer l'état "médiocre". Ceci évite des erreurs ultérieures si le problème provient d'un support défectueux.

Si l'erreur était due à un lecteur encrassé, nettoyez-le et vérifiez le support pour réinitialiser son état.

Si un support signalé comme médiocre figure dans un pool, il est recommandé d'en rechercher la cause. La fonction de vérification permet d'obtenir plus d'informations sur l'état de chaque support. Il est déconseillé de recycler simplement le support.

Création d'un pool de supports

Data Protector fournit des pools de supports par défaut, mais vous pouvez créer votre propre pool de supports en fonction de vos besoins.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Supports**, cliquez avec le bouton droit de la souris sur **Pools**, puis cliquez sur **Ajouter pool de supports** pour lancer l'assistant.
3. Dans la zone de texte Nom de pool, saisissez le nom du pool de supports, et dans la zone de texte Description, saisissez la description (facultatif). Sélectionnez ensuite dans la liste Type de support le type de support à utiliser avec le périphérique de sauvegarde. Cliquez sur **Suivant**.
4. Définissez les options comme suit :
   - Modifiez les valeurs par défaut des stratégies d'utilisation et d'allocation des supports (facultatif).
   - Pour utiliser un pool libre, activez l'option **Utiliser pool libre** et sélectionnez le pool libre dans la liste déroulante.
   - Pour désactiver la désallocation automatique de supports libres vers un pool libre, activez l'option Déplacer support libre vers pool libre.
   - Activez l'option **Support de magasin** si vous configurez un pool de support pour un

périphérique avec prise en charge de magasin. Vous ne pouvez pas utiliser cette option pour des pools libres.

Cliquez sur **Suivant**.

5. Modifiez les paramètres dans la boîte de dialogue Facteurs d'état des supports (facultatif).
6. Cliquez sur **Terminer** pour créer votre pool de supports et quitter l'assistant.

> **CONSEIL :**
> Il est possible de modifier un pool de supports déjà configuré. En revanche, il est impossible de modifier son type de support.

Modification d'un pool de supports

Vous pouvez modifier les propriétés d'un pool de supports pour l'adapter à vos besoins : vous pouvez modifier son nom, sa description, la stratégie d'utilisation et d'allocation des supports, ou les facteurs d'état des supports. En revanche, vous ne pouvez pas modifier le type de support.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Supports** et cliquez sur **Pools**.. La liste des pools de supports configurés s'affiche dans la zone de résultats.
3. Cliquez sur le nom du pool à modifier avec le bouton droit de la souris, puis sélectionnez **Propriétés**.
4. Dans la page de propriétés générales, vous pouvez modifier le nom du pool de supports dans la zone de texte Nom de pool, ou sa description dans la zone Description.
5. Cliquez sur l'onglet **Allocation** pour modifier les paramètres des stratégies d'utilisation et d'allocation des supports, pour activer ou désactiver l'utilisation d'un pool libre, pour activer ou désactiver l'option **Déplacer support libre vers pool libre**, ou pour activer l'option **Support de magasin**.
6. Cliquez sur l'onglet **Condition** pour modifier les paramètres de la boîte de dialogue Facteurs d'état des supports ou pour attribuer des valeurs par défaut à ces facteurs.
7. Cliquez sur **Appliquer** pour confirmer.

Suppression d'un pool de supports

En supprimant un pool de supports de la configuration de Data Protector, vous ne pourrez plus l'utiliser pour les sauvegardes. Vous ne pouvez pas supprimer un pool de supports utilisé comme pool par défaut pour les périphériques de sauvegarde. Dans ce cas, changez de pool de supports par défaut pour tous les périphériques ou supprimez les périphériques.

Si vous essayez de supprimer un pool de supports qui n'est pas vide, il vous sera demandé de commencer par exporter ou déplacer tous les supports du pool.

> **IMPORTANT :**
> Si vous supprimez un pool de supports utilisé dans une spécification de sauvegarde, le pool est

supprimé de la spécification.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Supports** et cliquez sur **Pools**. La liste des pools de supports configurés s'affiche dans la zone de résultats.
3. Cliquez sur le pool à supprimer avec le bouton droit de la souris, puis cliquez sur **Supprimer**. Confirmez l'opération.

Le pool de supports n'apparaît plus dans la liste des pools configurés.

Cycle de vie des supports

Le cycle de vie d'un support commence par son utilisation et se termine lorsque son critère d'utilisation maximum est atteint. Les étapes du cycle de vie sont généralement les suivantes :

Préparation des supports pour la sauvegarde

Cela comprend le formatage ou l'initialisation des supports et leur attribution à un pool de supports, par formatage (supports inutilisés et supports non-Data Protector utilisés) ou importation (supports Data Protector utilisés). S'il s'agit de supports déjà utilisés, vous pouvez les recycler/déprotéger et les exporter.

Utilisation de supports pour la sauvegarde

L'utilisation repose notamment sur le mode de sélection des supports pour la sauvegarde, sur les facteurs d'état des supports sélectionnés (le nombre d'écrasements, par exemple), sur la manière dont les nouvelles sauvegardes sont ajoutées au support et sur la date d'expiration de la protection des données.

Mise au coffre des supports dans un emplacement sécurisé

La mise au coffre des supports recouvre leur préparation pour un stockage dans un emplacement sécurisé et leur stockage réel. Pour préparer la mise au coffre, vous devez définir les stratégies de protection du catalogue appropriées, créer la liste d'emplacements de mise au coffre, spécifier et changer l'emplacement des supports, éjecter les supports et, dans certains cas, analyser les périphériques.

Data Protector prend en charge la mise au coffre à différents niveaux :

- Stratégies de protection des données et du catalogue.
- Sélection et éjection faciles des supports d'une bibliothèque.
- Le champ situation des supports vous indique l'emplacement physique où sont stockés les supports.
- Rapport indiquant les supports utilisés pour sauvegarder au cours d'une période donnée.
- Rapport indiquant la spécification de sauvegarde ayant utilisé des supports spécifiques lors de la

sauvegarde.

- Rapport sur les supports stockés à un emplacement spécifique avec une protection de données expirant dans une période spécifique.
- Affichage de la liste des supports nécessaires à la restauration et des emplacements physiques où sont stockés ces supports.
- Filtrage des supports affichés selon des critères spécifiques, tels qu'heure écrite sur le support ou support dont la durée de protection a expiré.

Il est recommandé d'effectuer une copie des données sauvegardées en vue de leur mise au coffre et de conserver le support original sur site pour permettre une restauration. Data Protector permet la création interactive ou automatique de copies supplémentaires des données figurant sur le support.

mise hors service des supports

Lorsque le support expire (lorsque son critère d'utilisation maximum est dépassé), il est marqué comme Médiocre et n'est plus utilisé par Data Protector.

Types de supports

Le type d'un support qualifie sa catégorie physique, comme DDS ou DLT. Dans Data Protector, vous devez sélectionner le type de support approprié au moment de la configuration des périphériques ; Data Protector évalue alors l'espace disponible sur le support pour le pool de supports spécifié.

Types de supports pris en charge

Pour plus de détails sur les types de supports pris en charge, consultez les dernières matrices de support sur https://softwaresupport.hpe.com/

Qualité des supports

La qualité des supports est déterminante pour leur sélection dans le cadre d'une sauvegarde, car elle a une incidence sur la capacité à lire ou à écrire des données sur ceux-ci. Les supports en bon état sont sélectionnés en priorité par rapport aux supports d'état passable. Les supports d'état médiocre ne sont pas sélectionnés pour la sauvegarde.

L'état des supports est déterminé par l'un des facteurs d'état suivants :

- En bon état
- Passable
- Médiocre

Vous pouvez afficher la page des propriétés Infos d'un support pour connaître sa qualité (son état).

Vous pouvez changer les facteurs d'état utilisés pour déterminer l'état d'un support dans la page de propriétés Options des propriétés du pool de supports. Les nouveaux facteurs d'état des supports sont utilisés pour déterminer l'état de l'ensemble des supports du pool.

La qualité des supports permet de déterminer le besoin de les remplacer.

Erreur de périphérique et qualité des supports

Si une erreur se produit au niveau du périphérique pendant une sauvegarde, le support utilisé pour la sauvegarde avec ce périphérique se voit attribuer l'état "médiocre". Ceci évite des erreurs ultérieures si le problème provient d'un support défectueux.

Si l'erreur était due à un lecteur encrassé, nettoyez-le et vérifiez le support pour réinitialiser son état.

Si un support est signalé comme médiocre, il est recommandé d'en rechercher la cause. La fonction de vérification permet d'obtenir plus d'informations sur l'état de chaque support. Il est déconseillé de recycler simplement le support.

Sélection de supports pour une sauvegarde

Le système de gestion des supports Data Protector sélectionne automatiquement les supports les plus appropriés à la sauvegarde. Les critères de base de la sélection sont les suivants :

- Les supports dont l'état est médiocre ne sont pas sélectionnés pour une sauvegarde.
- Les supports dont l'état est passable sont utilisés uniquement en l'absence de support en bon état.
- Les supports en bon état sont utilisés en premier.
- Les supports sont toujours sélectionnés dans le pool spécifié. Si le pool ne contient pas de supports non protégés, Data Protector accède à un pool libre (s'il est configuré).

La sélection s'effectue également en fonction des facteurs suivants :

Stratégie d'allocation de supports

La stratégie d'allocation des supports vous permet de définir le mode de sélection des supports de sauvegarde. Vous pouvez spécifier une stratégie souple dans laquelle tout support approprié peut être utilisé pour la sauvegarde, ou une stratégie stricte dans laquelle un support spécifique doit être disponible dans un ordre prédéfini.

Préallocation de supports

Vous pouvez spécifier l'ordre dans lequel les supports d'un pool de supports seront utilisés pour la sauvegarde. Cet ordre est défini dans une liste appelée liste de préallocation.

Etat des supports

L'état des supports a également une influence sur le choix des supports pour la sauvegarde. Par exemple, un support en bon état est utilisé en priorité par rapport à un support dont l'état est passable. Un support dont l'état est médiocre n'est pas utilisé pour une sauvegarde.

Un support marqué comme passable sert uniquement s'il ne contient aucun objet protégé. Sinon, une demande de montage est émise pour un support libre.

Utilisation de supports

La stratégie d'utilisation des supports contrôle le mode d'ajout de nouvelles sauvegardes sur des supports déjà utilisés. Elle a également une incidence sur la sélection des supports pour la sauvegarde.

Limite

Il est impossible d'ajouter des sauvegardes à des supports utilisés avec des périphériques Travan.

Les supports avec ajout possible doivent être en bon état, contenir des objets protégés et ne pas être pleins. Lors d'une session de sauvegarde avec partage de charge faisant appel à plusieurs périphériques, le concept d'ajout possible s'applique de manière individuelle à tous les périphériques : chacun d'entre eux utilise un support avec ajout possible comme premier support de la session. Les sessions de sauvegarde qui ajoutent des données sur un même support ne doivent pas obligatoirement se rapporter à la même spécification de sauvegarde.

> **REMARQUE :**
> Si vous utilisez la possibilité d'ajout et si la sauvegarde requiert plusieurs supports, seul le premier support utilisé peut contenir des données sauvegardées lors d'une session précédente. Data Protector fait ensuite uniquement appel à des supports vides ou non protégés.

Ses options sont les suivantes : Ajout possible, Sans possibilité d'ajout ou Ajout possible aux incrémentales uniquement.

Vous pouvez créer des chaînes de restauration pour un client sur les supports. Ces supports ne vont contenir qu'une sauvegarde complète et les sauvegardes incrémentales associées au même client :

- Configurez un pool par client avec la stratégie d'utilisation des supports **Ajout possible aux incrémentales uniquement**
- Liez un pool différent à chaque client de la spécification de sauvegarde, ou créez une spécification distincte par client.

Sachez que la création de supports contenant uniquement des sauvegardes incrémentales est possible.

Facteurs de sélection des supports

Stratégie d'allocation	Allouer d'abord support non formaté	Ordre de sélection Data Protector
Stratégie souple	Éteint	1. Liste de préallocation (si précisé) 2. Ajout possible (tel que défini dans la stratégie d'utilisation) 3. Supports Data Protector non protégés 4. Support non formaté 5. Support passable
Stratégie souple	ON	1. Liste de préallocation (si précisé)

		2. Ajout possible (tel que défini dans la stratégie d'utilisation) 3. Support non formaté 4. Supports Data Protector non protégés 5. Support passable
Stratégie stricte	Non applicable	1. Liste de préallocation (si précisé) 2. Ajout possible (tel que défini dans la stratégie d'utilisation) 3. Supports Data Protector non protégés 4. Support passable

Utilisation de types de format de supports différents

Data Protector reconnaît et utilise deux types de format différents pour écrire des données sur un support :

- Data Protector (pour les périphériques de sauvegarde qui sont sous le contrôle direct de Data Protector)
- NDMP (pour les périphériques de sauvegarde qui sont connectés aux serveurs NDMP)

Ces deux types de format utilisent deux composants Agent de support Data Protector (Agent de support général ou Agent de support NDMP) pour communiquer avec les périphériques de sauvegarde.

Limites

- Les supports qui sont écrits par un type de format seront reconnus comme vierges ou comme étrangers par un périphérique de sauvegarde qui utilise un type de format différent.
- Vous ne pouvez pas sauvegarder des objets en utilisant des types de format différents sur le même support.
- Deux composants Agent de support Data Protector différents ne peuvent être installés sur le même système.
- Il est fortement recommandé d'utiliser des pools de supports pour des types de format de support différents.

Supports WORM

WORM (write once, read many = écriture unique, lectures multiples) est une technologie de stockage des données qui permet d'écrire des informations sur un support une seule fois et empêche le lecteur d'effacer les données. Les supports WORM sont par nature non réinscriptibles car ils servent à stocker les données que vous voulez protéger contre tout effacement accidentel.

Utilisation des supports WORM avec Data Protector

La détection des bandes WORM n'est prise en charge que sous Windows. Sur les autres plates-formes, Data Protector ne reconnaît pas la bande comme non réinscriptible et il la considère comme une bande normale. Lors d'une tentative d'écrasement de données sur un support WORM, les messages d'erreur suivants sont affichés :

```
Cannot write to device ([19] The media is write protected.)
```

```
Tape Alert [ 9]: You are trying to write to a write-protected cartridge.
```

Pour éviter ce problème, procédez comme suit :

- Attribuez le niveau de protection de sauvegarde Permanent aux supports WORM.
- Conservez les supports WORM et les supports réinscriptibles dans des pools de supports distincts.

Supports WORM pris en charge

Toutes les opérations de support de Data Protector sont prises en charge pour les supports WORM gérés. Pour obtenir la liste à jour des lecteurs de bande et des supports WORM pris en charge, consultez les dernières matrices de support à l'adresse https://softwaresupport.hpe.com/.

À propos du formatage de supports

Le formatage (initialisation) d'un support consiste à le préparer pour une utilisation avec Data Protector en enregistrant les informations le concernant (ID, description et emplacement) dans l'IDB, et à écrire ces informations sur le support lui-même (en-tête du support). Lorsque vous initialisez (formatez) des supports, vous devez également préciser à quel pool de supports ils appartiennent.

Formatage avec des blocs de remplissage

Vous pouvez agrandir la taille de l'en-tête du support et le remplir avec des données incompressibles : les blocs de remplissage. Cette opération s'avère utile lors de la création de copies de support. Les blocs de remplissage ne sont pas copiés vers le support cible. Cela permet d'éviter que le support cible atteigne la fin de la bande avant le support source.

Le remplissage de bande n'est pas nécessaire si vous copiez les données sauvegardées au moyen de la fonctionnalité de copie d'objets.

Le remplissage de bande est désactivé par défaut. Pour l'activer, définissez la variable `OB2BLKPADDING_n` du fichier `omnirc` sur le système auquel le périphérique de sauvegarde est connecté.

Quand formater un support ?

Vous devez formater un support avant de l'utiliser pour la sauvegarde. Toutefois, lorsque vous utilisez la stratégie d'allocation de support Souple pour le pool, il n'est pas nécessaire de formater le support au préalable. Si l'option globale `InitOnLoosePolicy` a pour valeur 1 (0 étant la valeur par défaut), Data Protector formate automatiquement les nouveaux supports en cas de sélection pour une sauvegarde.

Il faut formater les supports non Data Protector avant la sauvegarde.

Les supports Data Protector contenant des données protégées ne sont pas formatés tant que vous ne supprimez pas la protection ; ce n'est qu'après l'avoir supprimée que les anciennes données peuvent être écrasées.

Etiquette de supports

Lors du formatage, Data Protector identifie chaque support avec une étiquette de support unique et un ID support. Ces deux informations sont stockées dans l'IDB et permettent à Data Protector de gérer le support. L'étiquette de support est une combinaison de la description définie par l'utilisateur et du code-barres du support (si l'option **Utiliser un code-barres comme étiquette de support lors de l'initialisation** est sélectionnée pour la bibliothèque). Le code-barres est affiché sous la forme d'un préfixe de la description des supports. Par exemple, [CW8279]Défaut DLT_1 est une étiquette de support constituée de la description Défaut DLT_1 et du code-barres CW8279. Si vous le souhaitez, vous pouvez écrire le code-barres en tant qu'étiquette du support dans son en-tête sur la bande lors de l'initialisation.

Une fois que vous avez formaté un support, vous ne pouvez plus changer son étiquette ni son emplacement, qui sont écrits sur le support lui-même, à moins de le formater à nouveau (ce qui entraîne l'écrasement des données). Lorsque vous changez les propriétés d'un support, seules les informations contenues dans la base de données interne sont modifiées.

Vous pouvez modifier l'étiquette et exclure le code-barres, mais ceci est déconseillé. Dans ce cas, vous devez effectuer un suivi manuel du code-barres réel et de l'étiquette de support attribués au support.

Formats de supports reconnus

Data Protector reconnaît les formats courants des données se trouvant sur le support si ce dernier a déjà été utilisé par une autre application. Il n'est cependant pas recommandé de se fier à Data Protector pour la reconnaissance d'autres types de supports, car cette opération dépend des plates-formes que vous utilisez.

Pour avoir la certitude qu'aucun support Data Protector n'est écrasé, vous devez sélectionner la stratégie d'allocation de supports stricte.

Data Protector réagit différemment selon le format qu'il reconnaît, comme indiqué dans le tableau ci-dessous.

Catégories de format de supports Data Protector

Format de support	Comportement relatif à la sauvegarde	Opérations possibles
Inconnu ou nouveau (vierge)	Stratégie souple : utilisé pour la sauvegarde Stratégie stricte : non utilisé pour la sauvegarde	Formater les supports
Supports écrits en utilisant la compression, utilisé maintenant sans la compression	Stratégie souple : utilisé pour la sauvegarde	Formater les supports

	Stratégie stricte : non utilisé pour la sauvegarde	
Supports écrits sans utilisation de la compression, utilisé maintenant avec la compression	Stratégie souple : utilisé pour la sauvegarde Stratégie stricte : non utilisé pour la sauvegarde	Formater les supports
Etranger à Data Protector (provenant d'une autre cellule)	Non utilisé pour la sauvegarde	Importer ou forcer un format de supports
tar, cpio, OmniBack I, ANSI label	Non utilisé pour la sauvegarde (ne peut être garanti)	Forcer le formatage de supports
Supports Data Protector non protégés	Utilisé pour la sauvegarde	Exporter les supports
Supports Data Protector protégés	Ajouter sauvegardes	Recycler (déprotéger) les supports

REMARQUE :
En cas de tentative de lecture sur un support écrit avec compression matérielle à l'aide d'un périphérique ne la prenant pas en charge, Data Protector ne parvient pas à identifier le support et à lire les données. Le support est alors traité comme inconnu ou nouveau.

Formatage d'un support

Vous devez formater un support avant de l'utiliser pour la sauvegarde. Les supports Data Protector contenant des données protégées ne sont pas formatés tant que vous ne supprimez pas la protection ; ce n'est qu'après l'avoir supprimée que les données peuvent être écrasées.

REMARQUE :
Vous ne pouvez pas formater un périphérique de bibliothèque de fichiers tant que vous ne l'avez pas utilisé pour effectuer la première sauvegarde. En effet, avant la première sauvegarde, le périphérique ne contient aucun dépôt de fichier et vous ne pouvez pas en créer manuellement. Les dépôts de fichier créés durant la sauvegarde sont l'équivalent d'un support. Selon la stratégie d'allocation des supports applicable au pool de supports du périphérique de bibliothèque de fichiers, les nouveaux supports formatés sont automatiquement supprimés.

IMPORTANT :
Utilisez l'option **Forcer opération** pour formater les supports dans des formats reconnus par Data Protector (tar, OmniBack I, etc.) ou pour reformater des supports Data Protector.

Les supports Data Protector contenant des données protégées ne sont pas formatés tant que la protection n'a pas été supprimée.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Support**, puis cliquez sur **Pools**.

3. Dans la zone de résultats, cliquez avec le bouton droit sur le pool de supports auquel vous souhaitez ajouter le support, puis choisissez **Formater** pour ouvrir l'assistant.
4. Sélectionnez le périphérique dans lequel se trouve le support cible, puis cliquez sur **Suivant**.
5. Vous pouvez donner une **description** aux supports et spécifier leur emplacement (facultatif). Une fois cette opération effectuée, cliquez sur **Suivant**.
6. Spécifiez des options supplémentaires pour la session : vous pouvez sélectionner l'option **Éjecter support après opération** ou **Forcer opération**. Vous pouvez également sélectionner **Spécifier la taille du support** ou laisser l'option **par défaut** activée.
7. Cliquez sur **Terminer** pour lancer le formatage et quitter l'assistant.

Une fois le formatage terminé, le format du support est défini sur Data Protector.

Formatage de tous les supports d'un magasin

Vous devez formater un support avant de l'utiliser pour la sauvegarde. Les supports Data Protector contenant des données protégées ne sont pas formatés tant que vous ne supprimez pas la protection ; ce n'est qu'après l'avoir supprimée que les données peuvent être écrasées.

Conditions préalables

Pour formater tous les supports du magasin en une seule étape, utilisez un périphérique dont l'option **support de magasin** est sélectionnée.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Support**, puis cliquez sur **Pools**.
3. Dans la zone de résultats, double-cliquez sur le pool de supports de votre choix.
4. Cliquez avec le bouton droit sur **Magasins**, puis cliquez sur **Formater magasin** pour lancer l'assistant.
5. Sélectionnez le lecteur de la bibliothèque qui effectuera l'opération, puis cliquez sur **Suivant**.
6. Vous pouvez donner une description aux nouveaux supports et spécifier leur emplacement (facultatif). Une fois cette opération effectuée, cliquez sur **Suivant**.
7. Spécifiez des options supplémentaires pour la session : vous pouvez utiliser l'option **Forcer opération** et sélectionner l'option **Spécifiez la taille du support** ou laisser l'option **Par défaut** activée.
8. Cliquez sur **Terminer** pour lancer le formatage et quitter l'assistant.

Une fois le formatage terminé, le format du support est défini sur Data Protector.

Formatage d'un seul support de magasin

Vous devez formater un support avant de l'utiliser pour la sauvegarde. Les supports Data Protector contenant des données protégées ne sont pas formatés tant que vous ne supprimez pas la protection ; ce n'est qu'après l'avoir supprimée que les données peuvent être écrasées.

Conditions préalables

Pour formater un support du magasin, utilisez un périphérique dont l'option **support de magasin** est sélectionnée.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Support**, puis cliquez sur **Pools**.
3. Dans la zone de résultats, cliquez avec le bouton droit sur le pool de supports auquel vous souhaitez ajouter le support, puis choisissez **Formater** pour ouvrir l'assistant.
4. Sélectionnez le périphérique et l'emplacement dans lequel se trouve le support cible, puis cliquez sur **Suivant**.
5. Vous pouvez donner une description au nouveau support et spécifier son emplacement (facultatif). Une fois cette opération effectuée, cliquez sur **Suivant**.
6. Spécifiez des options supplémentaires pour la session : vous pouvez utiliser l'option **Forcer opération** et sélectionner l'option **Spécifiez la taille du support** ou laisser l'option **Par défaut** activée.
7. Cliquez sur **Terminer** pour lancer le formatage et quitter l'assistant.

Une fois le formatage terminé, le format du support est défini sur Data Protector.

Formatage de supports d'un périphérique de bibliothèque

Vous devez formater un support avant de l'utiliser pour la sauvegarde. Les supports Data Protector contenant des données protégées ne sont pas formatés tant que vous ne supprimez pas la protection ; ce n'est qu'après l'avoir supprimée que les données peuvent être écrasées.

Si vous utilisez un périphérique de bibliothèque, vous pouvez sélectionner plusieurs emplacements avec la touche Ctrl et formater plusieurs supports à la fois.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez Périphériques et le périphérique de bibliothèque, puis cliquez sur **Emplacements**.
3. Dans la zone de résultats, cliquez avec le bouton droit sur les emplacements contenant les supports à formater, puis choisissez **Formater** pour ouvrir l'assistant.
4. Sélectionnez le lecteur de la bibliothèque qui effectuera l'opération, puis cliquez sur **Suivant**.
5. Sélectionnez le pool de supports auquel vous souhaitez ajouter les supports formatés, puis cliquez sur **Suivant**.
6. Vous pouvez donner une **description** au support et spécifier son emplacement (facultatif). Une fois cette opération effectuée, cliquez sur **Suivant**.
7. Spécifiez des options supplémentaires pour la session : vous pouvez utiliser l'option **Forcer opération** et sélectionner l'option **Spécifiez la taille du support** ou laisser l'option **Par défaut**

activée.

8. Cliquez sur **Terminer** pour lancer le formatage et quitter l'assistant.

Une fois le formatage terminé, le format du support est défini sur Data Protector.

À propos de l'importation de supports

L'importation de supports est l'action qui consiste à ajouter des supports Data Protector étrangers à une cellule à un pool de supports sans perdre les données qui se trouvent sur les supports. Le support doit avoir été préalablement exporté — ce qui veut dire qu'il provient d'une autre cellule Data Protector.

L'importation de support consiste à écrire les informations relatives aux données sauvegardées sur le support dans la base de données interne afin de pouvoir les parcourir ultérieurement pour effectuer une restauration.

Points à prendre en considération

- Au cours de l'importation de support, les informations d'attributs, telles que la taille du support ou de l'objet, ne sont pas reconstituées et la taille affichée des objets importés est de 0 Ko.
- Selon le support et le périphérique de sauvegarde que vous utilisez, l'importation peut prendre un temps considérable.
- Vous ne pouvez pas importer de supports dans des pools libres.
- Si vous tentez d'importer une copie qui a été supprimée et que le support d'origine ne se trouve pas dans la base de données interne, vous devez soit importer tout d'abord le support d'origine à l'aide de l'option Forcer opération, soit en importer la copie à l'aide de l'option Importer la copie comme étant l'original.
- Lors de l'importation de supports WORM sur lesquels la protection des données a déjà expiré dans une cellule Data Protector, assurez-vous de spécifier une nouvelle valeur de protection des données à l'aide de l'option **Protection** (par défaut, la valeur est définie sur Permanente). Cela permet à Data Protector d'ajouter des données aux supports WORM.

Quand importer un support ?

La fonction d'importation est généralement utilisée pour déplacer un support d'une cellule Data Protector à une autre. Dans ce cas, les informations relatives à l'espace disponible sur le support ne sont pas mises à jour.

Nous vous recommandons d'importer en une seule fois tous les supports utilisés dans une session de sauvegarde. Si vous ajoutez seulement une partie des supports de la session en question, vous ne pourrez pas restaurer les données réparties sur les autres supports

Pour les périphériques de bibliothèque de fichiers, vous pouvez uniquement importer des dépôts de fichier qui appartenaient auparavant au périphérique et qui ont été exportés au préalable. Pour importer des supports à partir d'une bibliothèque de fichiers résidant sur un hôte autre que celui cible, vous devez le faire à destination d'un périphérique de bibliothèque de stockage de fichiers.

Importation d'un support

Importez des supports lorsque vous voulez ajouter des supports déjà utilisés par Data Protector dans un pool de supports afin de pouvoir parcourir les données à restaurer par la suite.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**.
3. Dans la zone de résultats, cliquez avec le bouton droit sur le périphérique vers lequel vous souhaitez importer un support, puis cliquez sur **Importer** pour ouvrir l'assistant.
4. Sélectionnez le pool de supports auquel vous souhaitez ajouter les supports importés, puis cliquez sur **Suivant**.
5. Sélectionnez l'option **Importer la copie en tant qu'original** et choisissez l'option **Journalisation** qui correspond à vos besoins (facultatif).
6. Cliquez sur **Terminer** pour démarrer l'importation et quitter l'assistant.

Le message Informations sur la session affiche l'état de l'opération d'importation. Une fois l'importation terminée, le format du support est défini sur Data Protector.

Importation de tous les supports d'un magasin

Importez des supports lorsque vous voulez ajouter des supports déjà utilisés par Data Protector dans un pool de supports afin de pouvoir parcourir les données à restaurer par la suite.

Conditions préalables

Pour importer tous les supports du magasin en une seule étape, utilisez un périphérique dont l'option **support de magasin** est sélectionnée.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Support**, puis cliquez sur **Pools**.
3. Dans la zone de résultats, cliquez deux fois sur le pool de supports dont les supports se trouvent dans le magasin. Les éléments Support et Magasin s'affichent.
4. Cliquez avec le bouton droit sur **Magasins**, puis cliquez sur **Importer magasin** pour lancer l'assistant.
5. Sélectionnez le lecteur de la bibliothèque qui effectuera l'opération, puis cliquez sur **Suivant**.
6. Spécifiez la description des nouveaux supports (facultatif) ou laissez l'option **Générer automatiquement** activée, puis cliquez sur **Suivant**.
7. Sélectionnez l'option **Importer la copie en tant qu'original** et choisissez l'option **Journalisation** qui correspond à vos besoins (facultatif).
8. Cliquez sur **Terminer** pour lancer l'importation et quitter l'assistant.

Le message Informations sur la session affiche l'état de l'opération d'importation. Une fois l'importation terminée, le format du support est défini sur Data Protector.

Importation d'un seul support de magasin

Importez un support déjà utilisé par Data Protector lorsque vous souhaitez ajouter le support à un pool de supports afin de pouvoir parcourir les données à restaurer par la suite.

Conditions préalables

Pour formater un support dans le magasin, utilisez un périphérique dont l'option **support de magasin** est sélectionnée.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Support**, puis cliquez sur **Pools**.
3. Dans la zone de résultats, cliquez deux fois sur le pool de supports dont le support se trouve dans le magasin. Les éléments Support et Magasin s'affichent.
4. Cliquez avec le bouton droit sur l'élément **Supports**, et cliquez ensuite sur **Importer** pour ouvrir l'assistant.
5. Sélectionnez le lecteur et l'emplacement dans la bibliothèque où se trouve le support cible, puis cliquez sur **Suivant**.
6. Sélectionnez l'option **Importer la copie en tant qu'original** et choisissez l'option **Journalisation** qui correspond à vos besoins (facultatif).
7. Cliquez sur **Terminer** pour démarrer l'importation et quitter l'assistant.

Le message Informations sur la session affiche l'état de l'opération d'importation. Une fois l'importation terminée, le format du support est défini sur Data Protector.

Importation de supports d'un périphérique de bibliothèque

Importez des supports lorsque vous voulez ajouter des supports déjà utilisés par Data Protector dans un pool de supports afin de pouvoir parcourir les données à restaurer par la suite.

Si vous utilisez un périphérique de bibliothèque, vous pouvez sélectionner plusieurs emplacements avec la touche Ctrl et formater plusieurs supports à la fois.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Périphériques** et le périphérique de bibliothèque, puis cliquez sur **Emplacements**.
3. Dans la zone de résultats, sélectionnez les emplacements contenant les supports à importer.
4. Cliquez avec le bouton droit sur les emplacements sélectionnés, puis cliquez sur **Importer** pour lancer l'assistant.
5. Sélectionnez le lecteur de bibliothèque sur lequel l'échangeur chargera les supports à importer,

puis cliquez sur **Suivant**.

6. Sélectionnez le pool de supports auquel vous souhaitez ajouter les supports importés, puis cliquez sur **Suivant**.
7. Sélectionnez l'option **Importer la copie en tant qu'original** et choisissez l'option Journalisation qui correspond à vos besoins (facultatif).
8. Cliquez sur **Terminer** pour lancer l'importation et quitter l'assistant.

Le message Informations sur la session affiche l'état de l'opération d'importation. Une fois l'importation terminée, le format du support est défini sur Data Protector.

Exportation et importation de supports avec sauvegardes cryptées

Pour restaurer des données d'une sauvegarde cryptée vers un client dans une cellule Data Protector différente, vous devez importer les supports et les clés de cryptage dans le Gestionnaire de cellule de destination conformément aux instructions suivantes.

> **REMARQUE :**
> Data Protector permet également de gérer manuellement les clés de cryptage (expiration, réactivation, exportation, importation et suppression des clés) via l'interface de ligne de commande (CLI). Pour plus d'informations, reportez-vous à la page de manuel `omnikeytool` ou à la *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Environnement Gestionnaire de cellule ou environnement MoM sans CMMDB

Dans un environnement Gestionnaire de cellule ou MoM dans lequel des MMDB locales sont utilisées, suivez les étapes ci-dessous pour exporter et importer un support avec sauvegarde cryptée :

Procédure

1. Sur le Gestionnaire de cellule d'origine, exportez le support depuis l'IDB. Cette opération exporte aussi les clés de cryptage pertinentes de la banque de clés vers le fichier *`mediumID`*`.csv`, dans le répertoire des clés de cryptage exportées par défaut.
2. Transférez le fichier *`mediumID`*`.csv` vers le Gestionnaire de cellule de destination et placez-le dans le répertoire des clés de cryptage importées par défaut.
3. Insérez le support exporté dans le lecteur qui sera utilisé par le Gestionnaire de cellule de destination.
4. Dans le Gestionnaire de cellule de destination, importez le support. Lors de cette opération, les clés sont également importées depuis le fichier *`mediumID`*`.csv`.

> **REMARQUE :**
> Si le fichier des clés est manquant, vous pouvez néanmoins importer le support, mais l'importation du catalogue ne peut pas être effectuée en raison de l'absence des clés de décryptage.

Environnement MoM avec CMMDB

Dans un environnement MoM dans lequel la CMMDB est utilisée, toutes les informations relatives aux supports sont stockées dans le Gestionnaire MoM, mais les ID des clés de cryptage utilisés par ces supports ainsi que la CDB sont stockés dans une banque de clés locale dans chaque Gestionnaire de cellule. Notez que toutes les opérations de gestion des supports doivent être réalisées dans le Gestionnaire de cellule MoM.

Pour exporter et importer un support avec sauvegarde cryptée lorsque la CMMDB réside dans le Gestionnaire MoM, procédez comme suit :

Procédure

1. Exportez le support à partir de la CMMDB Les ID des clés sont exportés vers le fichier *mediumID*.csv, dans le répertoire des clés de cryptage exportées par défaut.
2. Transférez le fichier *mediumID*.csv vers le Gestionnaire de cellule de destination et placez-le dans le répertoire des clés de cryptage importées par défaut.
3. Depuis le Gestionnaire MoM, éjectez un support d'une bibliothèque.
4. Déplacez un support du pool de supports d'origine au pool de supports de destination qui est associé à un lecteur dans la cellule de destination. Lors de cette opération, le catalogue est également importé.
5. Insérez le support exporté dans le lecteur qui sera utilisé par le Gestionnaire de cellule de destination.
6. Dans le Gestionnaire de cellule de destination, importez le support. Lors de cette opération, les clés sont également importées depuis le fichier *mediumID*.csv.

À propos de la copie de supports

La fonctionnalité de copie de supports Data Protector vous permet de copier des supports après l'exécution d'une sauvegarde. La procédure de copie d'un support consiste à créer une copie exacte d'un support de sauvegarde. Vous pouvez placer les copies ou les supports originaux en lieu sûr à des fins d'archivage/de mise au coffre, et conserver l'autre jeu de supports sur site à des fins de restauration.

Conditions préalables

Vous devez utiliser deux périphériques, un pour un support source et l'autre pour un support cible. Vous pouvez également copier des supports se trouvant dans des périphériques de bibliothèque possédant plusieurs lecteurs. Dans ce cas, utilisez un lecteur pour le support source et un autre pour le support cible.

- Les supports sources et cibles doivent être de même type.
- Si vos supports cibles sont des supports Data Protector contenant des données protégées, vous devez d'abord les recycler, puis les formater.

Limites

- Vous pouvez réaliser plusieurs copies (supports cibles) d'un support (support source), mais vous ne pouvez pas copier des copies de supports.
- Vous ne pouvez copier que des supports résidents Data Protector (supports dans des périphériques).
- Etant donné que la copie de supports est conçue pour réaliser des copies exactes de supports généralement déplacés à un autre endroit, elle ne fonctionne pas avec les bibliothèques de fichiers. Pour copier les données d'une bibliothèque de fichiers, utilisez la fonction de copie d'objets.
- La copie de supports n'est pas disponible pour ses supports qui se trouvent dans des pools libres.
- La simultanéité des périphériques NAS contrôlés par un serveur NDMP est limitée à 1.
- La copie des supports n'est pas prise en charge pour les sessions de sauvegarde NDMP Celerra.

Quand copier un support ?

Vous pouvez copier un support dès la fin de la session de sauvegarde. Cependant, vous devez tenir compte de la disponibilité des périphériques qui seront utilisés pour la copie des supports. Il est recommandé d'attendre la fin de toutes les sauvegardes utilisant des périphériques spécifiques avant d'utiliser ces périphériques pour la copie de supports.

Résultats de la copie d'un support

La copie de supports aboutit à deux jeux de supports identiques : le jeu de supports originaux et la copie. Vous pouvez utiliser l'un des deux jeux pour la restauration.

Après que le support source a été copié, Data Protector le marque comme sans possibilité d'ajout pour empêcher l'ajout de nouvelles sauvegardes. (Cela résulterait en une différence entre l'original et sa copie). La copie est aussi marquée comme non utilisable.

Restauration à partir d'une copie

Par défaut, Data Protector restaure les données du jeu de supports d'origine. Toutefois, si ce jeu n'est pas disponible, mais qu'une copie l'est, elle sert à la restauration.

Si le périphérique ne dispose ni de l'original ni d'une copie lors de la restauration, Data Protector émet une demande de montage en affichant à la fois l'original et la copie comme supports nécessaires à la restauration. Vous pouvez utiliser l'un ou l'autre.

Si vous employez un périphérique autonome pour la restauration, vous pouvez décider d'effectuer l'opération à partir de la copie plutôt qu'à partir de l'original. Pour cela, insérez la copie dans le périphérique à utiliser pour la restauration, ou sélectionnez le périphérique contenant la copie. Toutefois, si vous effectuez une restauration à l'aide d'un périphérique de bibliothèque contenant l'original, Data Protector l'utilise pour l'opération.

> **REMARQUE :**
> Lors de la copie de supports, il est possible que le support cible atteigne la fin de la bande avant le support source. Cela se produit lorsque le support source a été écrit en mode continu et que vous effectuez une copie sur un système occupé ou via un réseau chargé, ce qui peut créer des

> espaces vides à l'endroit où la bande a stoppé et a redémarré. Vous pouvez prévenir ce problème en activant le remplissage de bande lorsque vous formatez des supports.

Copie d'un support

Vous pouvez copier des supports à des fins d'archivage ou de mise au coffre. Vous devez démarrer la copie de chaque support séparément, car un seul support peut être copié lors d'une session de copie de support.

Copie d'un support dans un périphérique autonome

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Périphériques**, cliquez avec le bouton droit sur le périphérique contenant le support à copier, puis cliquez sur **Copier**.
3. Sélectionnez le périphérique (lecteur et emplacement dans la bibliothèque) où se trouve le support cible, puis cliquez sur **Suivant**.
4. Sélectionnez le pool de supports auquel vous souhaitez ajouter la copie du support, puis cliquez sur **Suivant**.
5. Spécifiez la description et l'emplacement de la copie du support, puis cliquez sur **Suivant**.
6. Spécifiez des options supplémentaires pour la session : vous pouvez sélectionner l'option **Forcer opération**, spécifier la taille du support et sa protection.

   > **CONSEIL :**
   > Utilisez l'option **Forcer opération** si le support cible a d'autres formats reconnus par Data Protector (tar, OmniBack I, etc.) ou s'il s'agit de supports Data Protector sans protection.

7. Cliquez sur **Terminer** pour lancer la copie et quitter l'assistant.

Le message Informations sur la session affiche l'état de l'opération de copie des supports.

Copie d'un support dans un périphérique de bibliothèque

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, sous **Supports**, développez **Pools**, puis développez le pool de supports contenant le support à copier. Cliquez avec le bouton droit sur le support, puis cliquez sur **Copier** pour ouvrir l'assistant.
3. Sélectionnez un lecteur pour le support à copier et cliquez sur **Suivant**. Cette étape est ignorée si la bibliothèque ne contient qu'un seul lecteur.
4. Sélectionnez le périphérique (lecteur et emplacement dans la bibliothèque) où se trouve le support cible, puis cliquez sur **Suivant**.
5. Sélectionnez le pool de supports auquel vous souhaitez ajouter la copie du support, puis cliquez sur **Suivant**.
6. Spécifiez la description et l'emplacement de la copie du support, puis cliquez sur **Suivant**.

7. Spécifiez des options supplémentaires pour la session : vous pouvez sélectionner l'option **Forcer opération**, spécifier la taille du support et sa protection.

   > **CONSEIL :**
   > Utilisez l'option **Forcer opération** si le support cible a d'autres formats reconnus par Data Protector (tar, OmniBack I, etc.) ou s'il s'agit de supports Data Protector sans protection.

8. Cliquez sur **Terminer** pour lancer la copie et quitter l'assistant.

Le message Informations sur la session affiche l'état de l'opération de copie des supports.

Copie automatisée des supports

La copie automatisée des supports est un processus automatique qui crée des copies des supports contenant des sauvegardes. Par rapport à la copie de supports lancée manuellement, il convient de tenir compte de la limite ci-après.

Limites

- Vous ne pouvez pas utiliser de périphériques autonomes pour la copie automatisée des supports mais seulement des périphériques de bibliothèque.

  Vous ne pouvez pas utiliser des périphériques Backup to Disk (B2D) pour la copie automatisée des supports.
- La copie automatisée des supports n'est pas prise en charge pour les sessions de sauvegarde NDMP Celerra.

Copie automatisée des supports

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

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

Les périphériques sont verrouillés au début de la session. Ceux qui ne sont pas disponibles à ce moment précis ne peuvent pas être utilisés durant la session car le verrouillage de périphérique est impossible après le début de la session. Notez qu'au moins une paire de périphériques doit être disponible pour chaque type de support afin de permettre à la session complète de se dérouler correctement. La session échoue s'il est impossible de verrouiller le nombre minimum de périphériques requis.

Le support source définit le pool de destination du support cible. Cela signifie que le support copié appartiendra au même pool que le support original.

La période de protection par défaut pour la copie est identique à celle de la protection pour l'original. Vous pouvez définir une période de protection différente lorsque vous créez ou modifiez la spécification de copie automatisée des supports.

La fonction de copie automatisée des supports ne gère pas les demandes de montage ou "cleanme". Si la fonction reçoit une demande de montage, elle cesse de prendre en compte la paire de supports concernée mais la session se poursuit. Vous pouvez copier manuellement les supports non copiés au terme de la session de copie automatisée.

En cas d'erreur de support, le périphérique concerné sera évité durant cette session de copie automatisée des supports. Cependant, si aucun autre périphérique n'est disponible, il sera réutilisé.

Types de copie automatisée des supports

Il existe deux types de copie automatisée des supports : la copie post-sauvegarde et la copie planifiée.

Copie de supports post-sauvegarde

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

Copie de supports planifiée

La copie de supports planifiée a lieu à l'instant défini par l'utilisateur. Les supports utilisés dans des spécifications de sauvegarde différentes peuvent être copiés dans une session unique. Pour définir les supports à copier, vous créez une spécification de copie automatisée des supports.

Configuration de la copie des supports post-sauvegarde

La copie post-sauvegarde des supports est un processus qui crée une copie d'un support utilisé dans une session de sauvegarde particulière au terme de cette session.

> **REMARQUE :**
> En cas d'abandon d'une session de sauvegarde, une session de copie de support post-sauvegarde démarre quand même, au cas où certains objets aient été sauvegardés.

Limites

- Vous ne pouvez utiliser que des périphériques de sauvegarde.
- Le support source et le support cible doivent être de même type.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Opérations automatisées** puis cliquez sur **Opération de support de post-sauvegarde** pour ouvrir l'assistant.
3. Dans la liste déroulante Spécification de sauvegarde, sélectionnez la spécification de sauvegarde dont vous voulez copier le support. Dans la liste déroulante Type opération support, sélectionnez **Copie de supports** et cliquez sur **Suivant**.

4. Sélectionnez les périphériques sources et les périphériques cibles qui seront utilisés. Pour chaque type de support, vous devez disposer d'une paire de périphériques au minimum (un périphérique source et un périphérique cible). Cliquez sur **Next**.
5. Spécifiez le nombre de copies, si le support est éjecté automatiquement après l'opération, ainsi que l'emplacement et la protection pour le support cible. Cliquez sur **Terminer** pour quitter l'assistant

Configuration de la copie des supports planifiée

La copie de supports planifiée est un processus qui crée une copie d'un support utilisé dans une session de sauvegarde particulière à un moment planifié. Vous pouvez planifier plusieurs opérations de copie dans une seule session. Les supports seront copiés simultanément si suffisamment de périphériques sont disponibles. Sinon, ils seront copiés séquentiellement.

Limites

- Vous ne pouvez utiliser que des périphériques de sauvegarde.
- Le support source et le support cible doivent être de même type.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur **Opérations automatisées**, puis cliquez sur **Ajouter opération de support planifiée** pour ouvrir l'assistant.
3. Dans la zone de texte Nom opération de support, tapez un nom pour l'opération. Dans la liste déroulante Type opération support, sélectionnez **Copie de supports** et cliquez sur **Suivant**.
4. Sélectionnez les périphériques sources et les périphériques cibles qui seront utilisés. Pour chaque type de support, vous devez disposer d'une paire de périphériques au minimum (un périphérique source et un périphérique cible). Cliquez sur **Suivant**.
5. Spécifiez la période dans laquelle vous voulez rechercher des sessions de sauvegarde. Cliquez sur **Suivant**.
6. Précisez les spécifications de sauvegarde des sauvegardes que vous voulez copier. Cliquez sur **Suivant**.
7. Spécifiez l'état et la protection requis du support source. Cliquez sur **Suivant**.
8. Spécifiez le nombre de copies, si le support est éjecté automatiquement après l'opération, ainsi que l'emplacement et la protection pour le support cible. Cliquez sur **Terminer** pour quitter l'assistant. Si vous le souhaitez, vous pouvez planifier la copie de supports à l'aide du planificateur.

   Pour plus d'informations sur la création et la modification de planifications dans Data Protector, voir *Planificateur, Page 110*.

   > **IMPORTANT :**
   > Avec Data Protector 10.00, les planificateur de base et avancé sont rendus obsolètes et remplacés par un nouveau planificateur Web. Vous pouvez configurer des sauvegardes sans surveillance en planifiant des sessions de sauvegarde à exécuter à des instants précis. Pendant la mise à niveau de Data Protector, toutes les planifications Data

Protector existantes sont automatiquement migrées vers le nouveau planificateur.

Analyse d'un périphérique

L'analyse d'un périphérique permet de mettre à jour les informations Data Protector relatives aux supports se trouvant dans le périphérique ou après le déplacement manuel des supports.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques & supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**.
3. Dans la zone de résultats, cliquez avec le bouton droit sur le périphérique que vous souhaitez analyser, puis sélectionnez **Analyser**.

Le message Informations sur la session affiche l'état de l'opération d'analyse.

Analyse de supports d'un périphérique de bibliothèque

Analysez les supports dans les emplacements sélectionnés d'une bibliothèque pour mettre à jour les informations Data Protector sur ces supports dans le périphérique.

Selon le nombre d'emplacements sélectionnés, l'analyse peut prendre un certain temps. Data Protector doit charger un support à partir de chaque emplacement dans un lecteur, puis lire l'en-tête des supports.

Vous pouvez sélectionner plusieurs emplacements avec la touche Ctrl et analyser plusieurs supports à la fois. En revanche, vous ne pouvez utiliser qu'un seul lecteur.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**.
3. Dans la zone de résultats, double-cliquez sur le périphérique de bibliothèque, puis sur **Emplacements**.
4. Dans la zone de résultats, sélectionnez les emplacements contenant les supports à analyser.
5. Cliquez avec le bouton droit sur les emplacements sélectionnés, puis cliquez sur **Effacer** pour ouvrir l'assistant.
6. Sélectionnez le lecteur de la bibliothèque sur lequel l'échangeur chargera le support à analyser.
7. Cliquez sur **Terminer** pour démarrer l'analyse et quitter l'assistant.

Le message Informations sur la session affiche l'état de l'opération d'analyse.

CONSEIL :
Si vous avez activé l'option Support de lecture de code barres, vous pouvez effectuer l'analyse rapide d'une bibliothèque SCSI-II à l'aide de l'option **Analyse code-barres**.

Analyse d'un lecteur d'un périphérique de bibliothèque

Analysez le lecteur d'un périphérique de bibliothèque pour mettre à jour les informations de Data Protector concernant les supports dans le lecteur.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**.
3. Dans la zone de résultats, cliquez avec le bouton droit sur le périphérique que vous souhaitez analyser, puis double-cliquez sur l'icône **Lecteurs.**
4. Cliquez sur le lecteur à analyser avec le bouton droit de la souris, puis sélectionnez **Analyser**.

Le message Informations sur la session affiche l'état de l'opération d'analyse.

Activation du support de lecture de codes-barres

Lorsqu'un périphérique de bibliothèque SCSI utilise des supports avec codes barres, Data Protector peut utiliser les codes barres à l'aide du support de code barres suivant :

- Reconnaissance des bandes nettoyantes avec préfixe CLN.
- Désignation des supports par leur code-barres. Data Protector affiche le code-barres des supports sous la forme d'un préfixe de la description des supports.
- Analyse rapide des supports se trouvant dans les emplacements du référentiel de la bibliothèque par l'utilisation des codes-barres de ces supports.

CONSEIL :
Si vous sélectionnez l'option **Utiliser un code-barres comme étiquette de support lors de l'initialisation** dans les propriétés de bibliothèque, l'option **Utiliser un code-barres** est activée par défaut dans les options de **description du support** lors de l'initialisation du support. Si vous ne sélectionnez pas cette option, l'option par défaut est Générer automatiquement. L'option par défaut est utilisée lorsque Data Protector formate automatiquement un support.

REMARQUE :
Tous les codes-barres d'une cellule doivent être uniques, indépendamment du type de support ou de l'existence de plusieurs bibliothèques.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez Périphériques, cliquez sur le périphérique de bibliothèque cible avec le bouton droit de la souris, puis sélectionnez **Propriétés**. La page Propriétés du périphérique de bibliothèque s'affiche.
3. Cliquez sur l'onglet **Contrôle**, puis sélectionnez l'option **Support de lecture de code-barres**.
4. Pour écrire le code-barres dans l'en-tête du support sur la bande chaque fois que vous initialisez un support dans cette bibliothèque, sélectionnez l'option **Utiliser un code-barres comme**

étiquette de support lors de l'initialisation.

5. Cliquez sur **Appliquer** pour confirmer.

Analyse des codes-barres d'un périphérique de bibliothèque

Vous pouvez utiliser l'option **Analyser code-barres** pour effectuer une analyse rapide d'une bibliothèque SCSI. Cette opération s'effectue beaucoup plus rapidement que l'analyse d'un référentiel sans la fonction de code-barres.

Conditions préalables

L'option **Support de lecture de code-barres** doit être activée.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez Périphériques, cliquez sur le périphérique de bibliothèque cible avec le bouton droit, puis cliquez sur **Analyser code-barres**.

Le message Informations sur la session affiche l'état de l'opération d'analyse de codes-barres.

Recherche et sélection de supports

Vous pouvez rechercher, puis sélectionner des supports dans un pool de supports ou dans un périphérique de bibliothèque. Vous pouvez également lister les supports à l'aide du rapport Liste des supports. Cette fonction permet de localiser et de sélectionner des supports spécifiques sans avoir à parcourir la liste complète des supports.

La sélection de support est particulièrement utile pour la mise au coffre, par exemple pour mettre au coffre tous les supports sur lesquels des données ont été écrites la semaine précédente.

Recherche et sélection de supports d'un pool de supports

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques & supports**.
2. Dans la fenêtre de navigation, développez l'élément **Support**, puis cliquez sur **Pools**.
3. Dans la zone de résultats, cliquez sur un pool de supports avec le bouton droit de la souris, puis cliquez sur **Sélectionner supports**. La boîte de dialogue correspondante s'affiche.
4. Recherchez et sélectionnez les supports en fonction de leur description, de leur emplacement, de la session, de la période et de la protection, ou utilisez l'option Combiner sélections.

Recherche et sélection de supports d'un périphérique de bibliothèque

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**.
3. Dans la zone de résultats, cliquez deux fois sur un périphérique de bibliothèque, cliquez sur **Emplacements** avec le bouton droit de la souris, puis cliquez sur **Sélectionner supports**. La boîte de dialogue correspondante s'affiche.
4. Recherchez et sélectionnez les supports en fonction de leur description, de leur emplacement, de la session, de la période et de la protection, ou utilisez l'option Combiner sélections.

Recherche de supports à l'aide du rapport Liste des supports

Procédure

1. Dans la liste de contexte, cliquez sur **Rapports**, puis cliquez sur l'onglet **Tâches**.
2. Dans la fenêtre de navigation, développez **Pools et supports**, puis cliquez sur **Liste de supports** pour ouvrir l'assistant.
3. Suivez les instructions de l'assistant et spécifiez les critères de votre recherche. Cliquez sur **Terminer** pour afficher les résultats de la recherche.

Liste de préallocation de supports pour la sauvegarde

Vous pouvez spécifier l'ordre dans lequel les supports d'un pool de supports seront utilisés pour la sauvegarde. Cet ordre est défini dans une liste appelée liste de préallocation. Vous définissez cette liste au moment où vous configurez une sauvegarde. La liste de préallocation vous permet de contrôler les supports utilisés pour une session de sauvegarde. Vous devez rapprocher la liste de préallocation avec les supports disponibles avant chaque sauvegarde.

Vous pouvez également définir une préallocation de supports lorsque vous utilisez la fonction de copie d'objets ou de consolidation d'objet.

Selon la stratégie d'allocation du pool de supports, Data Protector opère de deux façons différentes :

- Si la liste de préallocation est utilisée en combinaison avec la stratégie d'allocation de supports **stricte**, Data Protector doit pouvoir accéder aux supports d'un périphérique de sauvegarde dans l'ordre défini par la liste. Si les supports ne sont pas disponibles, Data Protector émet une demande de montage. Si les supports figurant dans la liste de préallocation sont chargés dans un échangeur SCSI, Data Protector traite la séquence de supports automatiquement.
- Si la liste de préallocation est utilisée en combinaison avec la stratégie d'allocation de supports **souple**,les supports indiqués dans la liste sont utilisés en priorité. S'ils ne sont pas disponibles, tout support approprié se trouvant dans la bibliothèque sera utilisé.

Préallocation de supports pour la sauvegarde

Les points suivants peuvent contenir des informations supplémentaires :

- Vous pouvez également définir une préallocation de supports lorsque vous utilisez la fonction de copie d'objets ou de consolidation d'objet.
- Un pool de supports de bibliothèque de fichiers a une stratégie d'utilisation de supports Sans possibilité d'ajout par défaut. Comme cette stratégie vous confère les avantages de la bibliothèque de fichiers, il n'est pas recommandé d'en changer pour utiliser la liste de préallocation pour les supports de périphérique de bibliothèque de fichiers.

Pour définir une préallocation de supports dans une spécification de sauvegarde enregistrée, procédez comme suit :

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**, puis le type de spécification approprié (par exemple système de fichiers). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez deux fois sur la spécification de sauvegarde appropriée, puis cliquez sur l'onglet **Destination**.
4. Dans la page Destination, cliquez avec le bouton droit sur le périphérique sélectionné pour la sauvegarde et cliquez sur **Propriétés**.
5. Dans la boîte de dialogue Propriétés du périphérique, sélectionnez l'élément souhaité dans la liste déroulante Pool de supports.
6. Sous Liste de préallocation, cliquez sur **Ajouter**.

   La liste des supports du pool sélectionné s'affiche.
7. Sélectionnez un support et cliquez sur **Ajouter**.
8. Répétez les étapes 6 et 7 pour tous les supports souhaités. Lorsque vous avez terminé, cliquez sur **OK** pour revenir à la page de propriétés Destination.
9. Répétez les étapes 4 à 8 si la sauvegarde utilise plusieurs périphériques.
10. Cliquez sur Appliquer pour enregistrer les modifications.

Recyclage d'un support

L'opération de recyclage de support (retrait de la protection) consiste à supprimer la protection de toutes les données sauvegardées se trouvant sur ces supports, ce qui permet à Data Protector d'écraser les données sur ceux-ci lors des sauvegardes ultérieures. Le recyclage ne modifie pas les données qui se trouvent sur le support ; cette opération indique uniquement à Data Protector que ces données ne sont plus protégées.

> **IMPORTANT :**
> Tenez compte de points suivants :
>
> - Le recyclage supprime la protection de tous les objets du support. La protection des données provenant du même objet et de la même session, et qui se trouvent sur d'autres supports, est également supprimée.
> - L'opération de recyclage n'est pas disponible pour les supports des pools libres.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Support**, puis cliquez sur **Pools**. La liste des pools de supports configurés s'affiche dans la zone de résultats.
3. Double-cliquez sur le pool de supports contenant le support à recycler.
4. Cliquez sur le nom du pool cible avec le bouton droit de la souris, puis sélectionnez **Recycler**. Vous pouvez sélectionner plusieurs supports en même temps avec les touches Ctrl ou Maj.

Une fois l'opération effectuée, la valeur de protection du support est Aucun.

Importation du catalogue à partir de supports

L'importation du catalogue à partir d'un support consiste à écrire des informations détaillées telles que les noms et les versions des fichiers dans la base de données interne, ce qui vous permet de parcourir les fichiers et les répertoires à restaurer.

Vous pouvez également utiliser l'option Importer catalogue si la protection du catalogue a expiré pour un objet particulier et que vous ne pouvez plus parcourir ses fichiers et répertoires. Si les informations détaillées concernant les supports spécifiés existent déjà dans la base de données interne, les données ne seront pas dupliquées.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Support**, puis cliquez sur **Pools**.
3. Dans la zone de résultats, cliquez deux fois sur le pool de supports contenant le support à partir duquel vous souhaitez importer le catalogue.
4. Cliquez sur le support avec le bouton droit de la souris, puis sélectionnez **Importer catalogue**.
5. S'il y a plusieurs lecteurs, sélectionnez le lecteur de bibliothèque vers lequel importer les supports, puis cliquez sur **Suivant**.
6. Choisissez l'option de **journalisation** qui répond le mieux à vos besoins**.**
7. Cliquez sur **Terminer** pour lancer l'importation et quitter l'assistant.

Le message Informations sur la session affiche l'état de l'opération d'importation. Une fois l'importation terminée, vous pouvez parcourir les fichiers et les répertoires à restaurer.

Vérification d'un support

L'opération de vérification d'un support permet de savoir si le format des données qu'il contient est correct et de mettre à jour les informations concernant ce support dans la base de données interne. Vous ne pouvez effectuer de vérification que sur les supports Data Protector résidents. Selon les supports et le périphérique de sauvegarde que vous utilisez, la vérification peut prendre un temps considérable.

Vous pouvez vérifier une copie de support avant de la mettre au coffre. Vous pouvez également vérifier le support pour contrôler que la sauvegarde est utilisable, si des erreurs ont été signalées lors de l'opération.

Lors de la vérification des supports, Data Protector effectue les opérations suivantes :

- Vérification des en-têtes Data Protector contenant les informations sur le support (identification de supports, description et emplacement).
- Lecture de tous les blocs du support et vérification de leur format.
- Si l'option **CRC (contrôle de redondance cyclique)** a été utilisée pour la sauvegarde, le logiciel recalcule le CRC et le compare à celui enregistré sur le support. Dans ce cas, les données de la sauvegarde elles-mêmes sont cohérentes dans chaque bloc. Ce niveau de contrôle offre une haute fiabilité.

  Si l'option Contrôle CRC n'a pas été utilisée et que la vérification aboutit, cela signifie que toutes les données du support ont été lues. Le support n'a pas provoqué d'erreur de lecture, l'état matériel de la bande étant alors au moins acceptable. Ce niveau de contrôle peut être considéré comme partiel.

Vérification d'un support dans un périphérique autonome

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Périphériques**, cliquez avec le bouton droit sur le périphérique contenant le support à vérifier, puis sélectionnez, puis cliquez sur **Vérifier**.
3. Dans la zone de résultats, vous pouvez sélectionner l'option **Éjecter support après opération**. Cliquez sur **Terminer** pour vérifier le support.

   Cette étape est ignorée dans le cas d'un périphérique de fichier autonome.

Le message Informations de session affiche l'état de la vérification.

Vérification d'un support dans un périphérique de bibliothèque

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Périphériques** et le périphérique de bibliothèque, puis développez **Emplacements**. Cliquez avec le bouton droit sur l'emplacement contenant le support à vérifier, puis sélectionnez **Vérifier**.
3. Dans la zone de résultats, sélectionnez un lecteur de bibliothèque pour l'exécution de la vérification, puis cliquez sur **Terminer**.

Le message Informations de session affiche l'état de la vérification.

Déplacement d'un support

Vous pouvez déplacer un support d'un pool de supports vers un autre du même type si vous souhaitez réorganiser les sauvegardes et redéfinir la fonction de chaque pool. Ceci est également utile si vous voulez utiliser le support avec le périphérique par défaut d'un autre pool.

> **REMARQUE :**
> Vous ne pouvez pas déplacer un support vers un pool libre. Si vous utilisez un pool libre, le

déplacement des supports s'effectue en deux temps (le comportement dépend des options de pool libre sélectionnées) :

- Lors de leur sélection (allocation) pour une sauvegarde, les supports sont déplacés d'un pool libre vers un pool ordinaire.
- Après l'expiration de leur protection, les supports sont déplacés d'un pool ordinaire vers un pool libre.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Support**, puis cliquez sur **Pools**.
3. Dans la zone de résultats, cliquez deux fois sur le pool de supports dans lequel se trouve le support à déplacer. La liste des supports du pool s'affiche.
4. Cliquez avec le bouton droit sur le support à déplacer, puis cliquez sur **Déplacer vers pool** pour ouvrir l'assistant. Vous pouvez sélectionner plusieurs supports en même temps avec les touches Ctrl ou Maj.
5. Sélectionnez le pool de supports vers lequel vous souhaitez déplacer les supports.
6. Cliquez sur **Terminer** pour déplacer le support et quitter l'assistant..

CONSEIL :
Pour déplacer des supports vers une autre cellule, exportez-les de la cellule d'origine, puis importez-les dans la cellule souhaitée.

Exportation d'un support

Lorsque vous souhaitez déplacer un support vers une autre cellule Data Protector, vous devez l'exporter. L'exportation supprime les informations relatives au support et le contenu de ce dernier de la base de données interne. Data Protector ne sait plus que ce support existe. Toutefois, les données du support restent inchangées.

REMARQUE :
Nous vous recommandons de ne pas exporter manuellement des supports vers des périphériques de sauvegarde sur disque (B2D) qui se reposent sur la maintenance quotidienne pour le nettoyage du stockage, en raison de la nature non triviale de l'exportation manuelle de tous les supports. Autorisez la maintenance quotidienne à nettoyer le stockage.

Si vous exportez un support original, mais gardez des copies de ce support, l'une des copies devient alors l'original.

IMPORTANT :
Avant d'exporter le support, vous devez supprimer sa protection en le recyclant.

Il est recommandé d'exporter tous les supports d'une même session de sauvegarde. Si les données de la session sont réparties sur plusieurs supports et que vous n'en exportez qu'un seul, il se peut que vous ne puissiez pas restaurer les données. Data Protector sait que des données existent toujours sur les supports, mais certains supports ne sont plus disponibles.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Support**, puis cliquez sur **Pools**.
3. Dans la zone de résultats, cliquez deux fois sur le pool de supports contenant le support à exporter. Cliquez ensuite sur le support avec le bouton droit, puis cliquez sur **Exporter**.
4. Confirmez l'opération.

Le support exporté n'apparaît plus dans la liste des supports du pool.

Copie des données des supports du catalogue dans le fichier MCF

La copie de données du catalogue relatives aux supports dans un fichier permet d'écrire des informations détaillées, telles que les noms et les versions de fichiers dans des fichiers MCF (media container format) qui résident sur le Gestionnaire de cellule, dans le répertoire *données_programme_Data_Protector*\Config\Server\export\mcf (systèmes Windows) ou /var/opt/omni/server/export/mcf (systèmes UNIX). Ces fichiers peuvent ensuite être importés dans un autre Gestionnaire de cellule Data Protector, dans lequel les données de catalogue relatives aux supports deviennent disponibles pour consultation.

Limites

- Vous pouvez uniquement sélectionner les supports Data Protector.
- Du fait de la nature de la bibliothèque de fichiers Data Protector, avec laquelle les supports ne peuvent pas être exportés d'une bibliothèque pour être importés dans une autre, évitez les opérations **Copier le catalogue dans un fichier** et **Importer le catalogue à partir d'un fichier** sur ces supports.

Recommandations

- Du fait de la possibilité d'une grande quantité de données de catalogue par support, il est recommandé de stocker les fichiers sur une partition ou un point de montage distinct.
- Vous pouvez réduire la taille des fichiers en définissant l'option globale EnableMCFCompression sur 1. La compression est désactivée par défaut.

Les points suivants peuvent contenir des informations supplémentaires :

- Les données de catalogue relatives aux supports ne sont pas supprimées du Gestionnaire de cellule d'origine.
- Cette opération crée un fichier MCF par support.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Supports**, puis **Pools**.
3. Développez le pool contenant le support dont vous souhaitez copier le catalogue.
4. Cliquez avec le bouton droit sur le support, puis choisissez **Copier le catalogue dans un**

fichier.

5. Indiquez le répertoire de sortie pour le fichier MCF, lequel contiendra les données de catalogue relatives aux supports.
6. Cliquez sur **Terminer** pour lancer la copie et quitter l'assistant.

Le fichier MCF exporté peut être transféré vers le Gestionnaire de cellule de destination.

> **CONSEIL :**
> Pour obtenir le même résultat, vous pouvez cliquer sur **Périphériques**, cliquer avec le bouton droit de la souris sur le périphérique sélectionné, puis exécuter les étapes 5 et 6.

Importation des données des supports du catalogue depuis les fichiers MCF

L'importation de copies de données du catalogue relatives aux supports à partir de fichiers MCF (media container format) provenant du Gestionnaire de cellule d'origine vous permet de parcourir les fichiers sur le Gestionnaire de cellule de destination.

Conditions préalables

- Assurez-vous que les fichiers MCF que vous souhaitez importer sont transférés à partir du Gestionnaire de cellule d'origine et accessibles sur le Gestionnaire de cellule actif.

Limites

- Après qu'un support a été importé à partir d'un fichier, il ne peut pas être utilisé par les opérations qui nécessitent la présence physique de supports (par exemple restauration, copie du support). Pour qu'un support soit pleinement utilisable pour les opérations de Data Protector, il doit être accessible physiquement et analysé au moyen de l'analyse du support Data Protector. Dans le cas contraire, une demande de montage est émise.

Les points suivants peuvent contenir des informations supplémentaires :

- Lorsque vous importez de nombreux catalogues de supports à partir des fichiers MCF, veillez à bien importer tous les supports qui font partie d'une chaîne de restauration.
- Vous pouvez importer différents types de supports provenant de divers pools de supports au cours d'une session.
- L'interface utilisateur graphique Data Protector affiche et autorise uniquement la sélection des fichiers à extension mcf. Les autres fichiers de l'arborescence sont masqués. Vous pouvez toutefois les sélectionner par l'intermédiaire de l'interface de ligne de commande. Pour plus d'informations, reportez-vous à la page de manuel `omnimm` ou à la *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. 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.

3. Spécifiez les fichiers MCF que vous souhaitez importer.
4. Spécifiez des options supplémentaires pour la session : par défaut, l'option **Importer dans le pool d'origine si possible** est sélectionnée. Vous pouvez sélectionner le préfixe des nouveaux pools ou l'option **Importer la copie comme étant l'original**.
5. Cliquez sur **Terminer** pour démarrer l'importation et quitter l'assistant.

Modification de la description de support

La description de support vous permet d'identifier les différents supports. Les informations sur l'emplacement sont écrites sur le support et enregistrées dans l'IDB (base de données interne). Lors du formatage de nouveaux supports, une description correspondante est ajoutée. Si les supports ont été formatés automatiquement lors d'une sauvegarde, vous pouvez modifier la description générée automatiquement afin de mieux l'adapter à vos besoins.

Lorsque vous modifiez une description de support, Data Protector modifie la description dans l'IDB, et non sur le support lui-même. Si vous exportez puis importez des supports, la description de la base de données interne est remplacée par celle des supports.

La partie descriptive de l'étiquette de support est également modifiée, mais la partie code-barres reste identique.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Support**, puis cliquez sur **Pools**.
3. Dans la zone de résultats, double-cliquez sur le pool de supports contenant la description à modifier. La liste des supports du pool s'affiche.
4. Cliquez avec le bouton droit sur le support dont vous souhaitez changer la description, puis choisissez **Propriétés** pour ouvrir la page de propriétés générales du support.
5. Dans la zone de texte Description, saisissez une nouvelle description pour le support.
6. Cliquez sur **Appliquer** pour confirmer.

Changement d'emplacement de support

Le fait de spécifier l'emplacement des supports vous permet de les localiser lorsqu'ils ne sont plus dans le périphérique. Les informations sur l'emplacement sont également stockées dans l'IDB. Vous devez spécifier l'emplacement du support lors de son initialisation et le modifier chaque fois que vous déplacez le support (mise au coffre), par exemple pour le stocker hors site ("étagère 4 - boîte 3").

L'endroit où se trouve le support n'est jamais indiqué dans son en-tête.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez l'élément **Support**, puis cliquez sur **Pools**.
3. Dans la zone de résultats, double-cliquez sur le pool de supports contenant l'emplacement à modifier. La liste des supports du pool s'affiche.

4. Cliquez avec le bouton droit sur le support dont vous souhaitez changer l'emplacement, puis choisissez **Déplacer** pour ouvrir l'assistant.
5. Spécifiez un nouvel emplacement pour le support.
6. Cliquez sur **Terminer** pour quitter l'assistant

Création d'une liste d'emplacements

Vous pouvez créer une liste des emplacements de mise au coffre prédéfinis que vous utilisez fréquemment. Vous aurez accès à cette liste au moment de choisir un emplacement pour un support spécifique lorsque vous effectuerez une tâche de gestion de support (le formatage d'un support, par exemple).

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans le menu Edition, cliquez sur **emplacements**.
3. Spécifiez l'emplacement souhaité, puis cliquez sur le bouton **Ajouter**. Répétez cette opération pour spécifier plusieurs emplacements.
4. Cliquez sur **Terminer**.

Définition de la priorité d'emplacement des supports

Si une version d'objet que vous voulez restaurer, copier, consolider ou vérifier existe sur plusieurs jeux de supports, vous pouvez utiliser n'importe quel jeu de supports. Par défaut, Data Protector sélectionne automatiquement le jeu de supports le plus approprié. Vous pouvez influencer la sélection d'ensemble de supports par spécification de la priorité d'emplacement de supports.

Dans les cas où plusieurs jeux de supports répondent aux conditions de l'algorithme de sélection de jeu de supports, Data Protector utilisera le jeu de supports qui a le plus haut niveau de priorité (`1` est le plus haut niveau de priorité, `None` est le plus bas).

La priorité d'emplacement des supports peut être modifiée au niveau de la session de restauration, de copie d'objets, de consolidation ou de vérification d'objet.

Les points suivants peuvent contenir des informations supplémentaires :

- Par défaut, la priorité d'emplacement des supports n'est considérée que si plusieurs jeux de supports sont équivalents. Pour que la priorité d'emplacement des supports supplante tout autre critère de sélection, définissez l'option globale `UserSpecifiedMediaPriorityHasHigherImportance` sur 1.
- Pour que la priorité d'emplacement des supports soit effective, vous devez spécifier l'emplacement de chaque support. Vous pouvez le faire pour un seul ou pour plusieurs supports.
- La priorité d'emplacement des supports ne prend pas en compte les copies obtenues à l'aide de la fonctionnalité de copie des supports. Ces copies ne sont utilisées que si le support d'origine (celui qui a été utilisé comme source pour la copie) n'est pas disponible ou pas utilisable.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Supports** et cliquez sur **Emplacements**.
3. Dans la zone de résultats, cliquez deux fois sur un emplacement pour afficher ses propriétés.
4. Dans la liste déroulante **Priorité pour l'emplacement**, sélectionnez l'un des nombres disponibles (1 correspond à la priorité la plus élevée).
5. Cliquez sur **Appliquer** pour confirmer votre sélection.

Mise au coffre d'un support

Il est recommandé d'effectuer une copie des données sauvegardées en vue de leur mise au coffre et de conserver le support original sur site pour permettre une restauration. Data Protector permet la création interactive ou automatique de copies supplémentaires des données figurant sur le support.

Conditions préalables

- Vous devez définir les stratégies de protection de données et de protection du catalogue souhaitées lors de la configuration d'une spécification de sauvegarde.
- Vous devez configurer un coffre dans Data Protector. Utilisez un nom indiquant l'emplacement physique de stockage des supports.

Procédure

1. Dans le Gestionnaire Data Protector, modifiez l'emplacement des supports que vous voulez stocker.
2. Ejectez les supports du périphérique, puis stockez-les dans le coffre.

Effacement d'un support

Cette fonction n'est disponible que pour les disques magnéto-optiques. Elle vous permet d'effacer un disque magnéto-optique avant une session de sauvegarde, ce qui augmente la vitesse de la sauvegarde.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques & supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**.
3. Dans la zone de résultats, cliquez deux fois sur le périphérique magnéto-optique contenant le support à effacer.
4. Cliquez avec le bouton droit sur le support, puis cliquez sur **Effacer** pour ouvrir l'assistant.
5. (Facultatif) Sélectionnez l'option **Ejecter support après opération**.
6. Cliquez sur **Terminer** pour effacer le support et quitter l'assistant..

Le message Informations sur la session affiche l'état de l'opération d'effacement.

Détection des supports protégés en écriture

Data Protector peut détecter et traiter un support qui a été protégé mécaniquement par activation d'un commutateur de protection en écriture.

Les opérations suivantes peuvent détecter et traiter les supports protégés en écriture :

- Opérations en lecture seule telles que listage, analyse et vérification. Les opérations en lecture seule détectent les supports protégés en écriture et sont réalisées sans avertissement.
- Les opérations d'écriture, telles qu'initialisation, effacement et sauvegarde. Les opérations d'écriture détectent les supports protégés en écriture et abandonnent la session ou ignorent ces supports. Les sessions de sauvegarde traitent les supports protégés en écriture en tant que supports inutilisables et se comportent conformément à la stratégie d'allocation de supports. Si la stratégie d'allocation est stricte, une demande de montage est générée. Si la stratégie d'allocation est souple, alors le support est ignoré.

La détection d'un support protégé en écriture et toute modification de l'état de la protection en écriture sont consignés dans le fichier `media.log`.

> **REMARQUE :**
> Il est recommandé de ne pas utiliser des supports protégés en écriture avec Data Protector.

À propos des demandes de montage

Une demande de montage est un écran qui vous invite à insérer un support dans un périphérique. Une fois que vous avez répondu à la demande de montage en fournissant le support requis, la session se poursuit.

Data Protector émet une demande de montage dans les cas suivants :

- Le support spécifié n'est pas disponible. Cette situation peut se produire lorsqu'une liste de préallocation est utilisée pour la sauvegarde ou lorsque des supports nécessaires à la restauration sont manquants.
- Aucun support approprié n'est disponible. Cela peut se produire si les supports d'un pool qui se trouvent actuellement dans la bibliothèque ne sont pas appropriés, ou si le support dans un périphérique autonome n'est pas approprié, ou encore si le périphérique est vide.
- Le logement de bande est ouvert. Dans ce cas, refermez-le.

Les supports les plus appropriés pour la sauvegarde sont sélectionnés automatiquement par Data Protector. Vous devez être attentif à la façon dont les supports sont sélectionnés pour la sauvegarde.

À propos de la gestion de supports spécifique aux bibliothèques

Data Protector met à votre disposition des tâches de gestion de supports spécifiques pour des périphériques complexes tels que les bibliothèques afin de simplifier la gestion d'un grand nombre de supports.

Certaines tâches suivent la procédure standard comme, par exemple, la sélection, la copie, le recyclage ou le déplacement de support, ainsi que le changement d'emplacement de support. D'autres

tâches, telles que l'ajout ou la suppression d'un emplacement, ainsi que l'insertion, l'éjection, la vérification, le formatage, l'importation, l'analyse ou l'effacement de supports, peuvent dépendre du type de périphérique utilisé.

Dans les bibliothèques avec prise en charge de la lecture des codes-barres, Data Protector peut générer des descriptions de supports sur la base des codes-barres et les écrire dans l'en-tête de la bande lors de l'initialisation.

Utilisation de supports de bibliothèque par d'autres applications

Le support d'une bibliothèque (en particulier dans de très grandes bibliothèques telles que ADIC/GRAU et StorageTek) peut être utilisé par de nombreuses applications, et pas uniquement par Data Protector. Vous devez donc savoir quelles applications utilisent quels supports pour éviter qu'elles ne soient écrasées.

Idéalement, vous utiliserez la bibliothèque avec Data Protector exclusivement et laisserez Data Protector gérer l'ensemble de la bibliothèque. Cependant, si certaines de vos applications utilisent la bibliothèque, vous devez veiller à attribuer à Data Protector et aux autres applications des sous-ensembles de supports qui ne se chevauchent pas. Data Protector gère sa propre stratégie d'allocation de supports indépendante. Cela signifie que si un support spécifique a été attribué à Data Protector (ajouté à un pool de supports Data Protector), il reste sous le contrôle de Data Protector durant sa durée de vie ou jusqu'à ce qu'il soit supprimé du pool de supports Data Protector.

> **IMPORTANT :**
> Pour chaque type de support, vous devez configurer une bibliothèque dans Data Protector. Alors qu'un système ADIC/GRAU ou StorageTek peut stocker de nombreux types de supports physiquement différents, Data Protector peut seulement reconnaître une bibliothèque contenant un seul type de support. Par conséquent, vous devez créer une bibliothèque Data Protector pour chaque type de support du système.

Ce qui suit peut être utile :

- Utilisez les commandes Data Protector pour gérer les supports dans les bibliothèques ADIC/GRAU DAS et StorageTek. Si vous gérez les supports manuellement à l'aide des commandes ADIC/GRAU DAS ou StorageTek ACS, Data Protector ne pourra pas effectuer le suivi des changements d'emplacement ou d'informations sur les supports.
- Gérez l'ensemble de la bibliothèque à l'aide de Data Protector. Vous bénéficiez ainsi d'un point d'administration unique, d'où vous pouvez gérer les supports Data Protector et non Data Protector dans la bibliothèque.
- Créez au moins un pool de supports pour chaque type de support, par exemple, un pour le type 4mm et un pour le type 3480. Selon votre environnement, vous pouvez créer d'autres pools, par exemple, un par service.
- Vérifiez que Data Protector et les autres applications n'utilisent pas le même jeu de supports.

À propos de l'opération de requête HPE Data Protector utilisée avec des bibliothèques ADIC/GRAU DAS ou STK ACS

Lorsque l'opération de requête Data Protector est lancée, tous les supports configurés sur le serveur de bibliothèque DAS ou ACS sont interrogés, même si ces supports sont configurés dans Data Protector comme appartenant à plusieurs bibliothèques DAS ADIC/GRAU ou ACS STK logiques (pour la même bibliothèque physique). De plus, l'opération de requête Data Protector interroge également les supports configurés sur le serveur de bibliothèque DAS ou ACS pour être utilisés avec des applications autres que Data Protector. Par conséquent, une fois que l'opération de requête a été lancée à partir de Data Protector, les supports appartenant à d'autres bibliothèques DAS ADIC/GRAU ou ACS STK logiques que celle pour laquelle l'opération de requête a été lancée sont déplacés vers la bibliothèque DAS ADIC/GRAU ou ACS STK logique pour laquelle l'opération de requête a été lancée.

Il n'est ainsi par recommandé d'utiliser l'opération de requête Data Protector avec des bibliothèques DAS ADIC/GRAU ou ACS STK. Il est conseillé d'ajouter les volsers manuellement à l'aide de l'opération d'ajout de volsers de Data Protector au lieu de synchroniser l'IDB à l'aide de l'opération de requête Data Protector.

> **REMARQUE :**
> Les informations de cette section ne s'appliquent pas aux bibliothèques DAS ADIC/GRAU lorsque les bibliothèques logiques ne sont pas configurées à l'aide de Data Protector, mais avec les utilitaires DAS ADIC/GRAU. Si plusieurs bibliothèques logiques sont configurées à l'aide des utilitaires DAS ADIC/GRAU, l'opération de requête de Data Protector peut être appliquée en toute sécurité à ces bibliothèques.

Ajout d'un emplacement

Data Protector fournit une prise en charge complète de la gestion des emplacements et des supports dans les pools de supports utilisés par des bibliothèques. L'ajout d'un emplacement permet de localiser le support dans le périphérique de stockage.

Sur certaines bibliothèques, les emplacements sont détectés et ajoutés automatiquement lors de la configuration de la bibliothèque.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**.
3. Dans la zone de résultats, cliquez sur le nom de la bibliothèque avec le bouton droit, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Référentiel**, spécifiez l'emplacement à utiliser avec Data Protector, puis cliquez sur **Ajouter** pour ajouter l'emplacement à la liste. Utilisez un tiret pour spécifier plusieurs emplacement à la fois, 5-12 par exemple.

Veillez à utiliser un format supporté par votre bibliothèque. Par exemple, si vous ajoutez des emplacements à une bibliothèque SCSI, n'utilisez pas de lettres ou de zéros en tête.

5. Cliquez sur **Appliquer** pour confirmer.

Suppression d'un emplacement

Data Protector fournit une prise en charge complète de la gestion des logements et des supports dans les pools de supports utilisés par des bibliothèques. La suppression d'un emplacement empêche Data Protector d'utiliser et d'accéder à l'emplacement dans le référentiel. Les informations concernant l'emplacement sont supprimées de l'IDB.

La suppression des emplacements de supports n'est activée que pour les emplacements vides sur tout périphérique.

Cette opération n'affecte pas les volsers de la bibliothèque GRAU DAS, mais supprime seulement des supports spécifiques de l'IDB. Data Protector ignore donc l'existence de ces supports et ne les utilise pas.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**.
3. Dans la zone de résultats, cliquez sur le nom de la bibliothèque avec le bouton droit, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Référentiel**, sélectionnez l'emplacement à supprimer, puis cliquez sur **Supprimer**.
5. Cliquez sur **Appliquer** pour confirmer.

L'emplacement ne s'affiche plus dans la liste des emplacements.

Insertion d'un support

L'insertion d'un support signifie l'insérer physiquement dans un référentiel de bibliothèque et enregistrer les supports ajoutés comme membres de la bibliothèque.

Vous pouvez sélectionner l'emplacement de votre choix. L'introduction de supports n'affecte pas le pool de supports auquel ils appartiennent.

Pour insérer un support, il est recommandé de passer par l'interface utilisateur Data Protector. Si vous insérez manuellement un support avec les commandes du périphérique, les informations de la base de données interne ne sont plus cohérentes et vous devez analyser le périphérique pour mettre à jour ces informations.

> **CONSEIL :**
> Vous pouvez insérer plusieurs supports dans un périphérique d'un seul coup.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**. Une liste des périphériques configurés s'affiche dans la zone de résultats.
3. Dans cette zone, cliquez deux fois sur le nom de la bibliothèque.
4. Double-cliquez sur **Emplacements** pour afficher une liste des emplacements dans la zone de résultats.
5. Cliquez avec le bouton droit sur le ou les emplacements où vous voulez insérer le support, puis cliquez sur **Entrée** pour démarrer la session.

Il vous sera demandé d'insérer d'autres supports dans le périphérique selon le besoin.

Ejection d'un support

L'éjection d'un support correspond à son transfert physique de son emplacement dans le référentiel à la zone d'insertion/éjection (également appelée logement de bande) d'un périphérique de bibliothèque.

Pour éjecter les supports, il est recommandé d'utiliser le Gestionnaire Data Protector. Si vous éjectez manuellement un support avec les commandes du périphérique, les informations de la base de données interne ne sont plus cohérentes. Pour mettre à jour ces informations, vous devez analyser le périphérique.

S'il est impossible d'éjecter un support en raison d'un logement de bande occupé, Data Protector recommence l'opération jusqu'à ce que le logement soit libre ou jusqu'à l'expiration du délai prédéfini. Pendant ce processus, les robots sont accessibles à d'autres sessions.

Lors du processus d'éjection, aucune autre session ne peut utiliser les supports spécifiés.

Ejection de supports simultanée

Vous pouvez éjecter plusieurs supports d'une bibliothèque en une fois. Data Protector vous indique de retirer des supports d'un logement lorsqu'il est plein afin de libérer de l'espace pour d'autres supports à éjecter.

Ejection de supports prédéfinie

Avec certaines opérations, telles que la copie de support automatisée, vous pouvez spécifier si les supports seront éjectés automatiquement au terme de la session.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**. La liste des périphériques configurés s'affiche dans la zone de résultats.
3. Dans cette zone, cliquez deux fois sur le nom de la bibliothèque.
4. Double-cliquez sur l'élément **Emplacements** pour afficher la liste des emplacements dans la zone

de résultats.

5. Cliquez avec le bouton droit sur l'emplacement (ou les emplacements) souhaité(s), puis cliquez sur **Ejecter** pour ouvrir l'assistant.
6. Vous pouvez spécifier un autre emplacement pour le support (facultatif).
7. Cliquez sur **Terminer** pour éjecter le support et quitter l'assistant..

Le message Informations sur la session affiche l'état de l'opération d'éjection.

Effacement de support d'un périphérique de bibliothèque

Cette fonction n'est disponible que pour les disques magnéto-optiques. Vous ne pouvez l'utiliser qu'avant une session de sauvegarde, ce qui vous permet d'accélérer l'opération.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, cliquez sur **Périphériques**.
3. Dans la zone de résultats, cliquez deux fois sur le périphérique magnéto-optique contenant les supports à effacer. Les éléments Emplacements et Lecteurs s'affichent.
4. Double-cliquez sur **Emplacements**.
5. Cliquez avec le bouton droit sur les emplacements contenant les supports à effacer, puis cliquez sur **Effacer** pour ouvrir l'assistant.
6. Sélectionnez le lecteur de bibliothèque sur lequel l'échangeur doit charger les supports à effacer.
7. Cliquez sur **Terminer** pour effacer les supports et quitter l'assistant.

Le message Informations sur la session affiche l'état de l'opération d'effacement.

Ajout manuel de volsers

Avec des bibliothèques ADIC/GRAU DAS ou STK ACS, vous pouvez ajouter manuellement des volsers à une bibliothèque configurée dans Data Protector au lieu d'interroger la bibliothèque. Avec des bibliothèques DAS ADIC/GRAU ou ACS STK, lorsque plusieurs bibliothèques logiques sont configurées pour la même bibliothèque physique, il s'agit de la méthode recommandée pour ajouter des volsers à une bibliothèque configurée dans Data Protector. Avec les bibliothèques DAS ADIC/GRAU, cependant, lorsque les bibliothèques logiques ne sont pas configurées à l'aide de Data Protector, mais au contraire avec les utilitaires DAS ADIC/GRAU, l'opération de requête de Data Protector peut être utilisée en toute sécurité sur les bibliothèques (au lieu d'ajouter des volsers manuellement).

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, recherchez la bibliothèque à laquelle des volsers doivent être ajoutés et développez-la.
3. Cliquez avec le bouton droit sur **Emplacement**, puis sélectionnez **Ajouter volser(s)** dans le menu contextuel.

4. Dans la zone de texte Préfixe, entrez le préfixe du volser. Il est généralement composé de trois lettres.

   Dans la zone de texte De, saisissez le numéro de départ de la série de volsers à ajouter à la bibliothèque.

   Dans la zone de texte A, saisissez le numéro de fin de la série de volsers à ajouter à la bibliothèque.
5. Cliquez sur Terminer pour ajouter les volsers à l'IDB.

Interrogation des hôtes DAS ADIC/GRAU et ACSLM StorageTek

Pour obtenir des informations sur un référentiel dans les bibliothèques ADIC/GRAU ou StorageTek du serveur, vous pouvez interroger l'hôte (serveur) DAS ou ACSLM. Une requête répond avec le contenu de la base de données de support du serveur, puis synchronise les informations dans la base de données avec le contenu du référentiel.

Ceci est particulièrement utile si vous avez utilisé les commandes DAS GRAU ou ACS StorageTek pour gérer les supports, étant donné que cela entraîne des incohérences avec la base de données interne - Data Protector ne connaît pas le dernier état des supports dans le référentiel de bibliothèque.

Limite

L'analyse des volsers peut échouer si la bibliothèque ADIC/GRAU est configurée avec plus de 3970 volsers dans un même référentiel. Pour contourner ce problème, vous pouvez configurer plusieurs bibliothèques ADIC/GRAU logiques afin de diviser les différents emplacements du référentiel en plusieurs petits référentiels.

> **IMPORTANT :**
> Avec les bibliothèques DAS ADIC/GRAU et ACS STK, il n'est pas recommandé d'interroger le serveur DAS ou ACSLM STK lorsque plusieurs bibliothèques logiques sont configurées pour la même bibliothèque physique. Ajoutez les volsers manuellement. Avec les bibliothèques DAS ADIC/GRAU, cependant, lorsque les bibliothèques logiques ne sont pas configurées à l'aide de Data Protector, mais au contraire avec les utilitaires DAS ADIC/GRAU, l'opération de requête de Data Protector peut être utilisée en toute sécurité sur les bibliothèques.

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la liste des périphériques configurés, cliquez avec le bouton droit sur la bibliothèque que vous voulez interroger, puis cliquez sur **Requête**.

Cette action interroge l'hôte DAS ou ACSLM.

Chapitre 10: Sauvegarde

À propos de la sauvegarde

Une sauvegarde est une opération consistant à créer une copie des données du système sur un support de sauvegarde. Cette copie est stockée et conservée en vue d'une utilisation ultérieure pour le cas où l'original serait détruit ou endommagé.

Une session de sauvegarde est basée sur la spécification de sauvegarde et peut être lancée de manière interactive. Au cours d'une session de sauvegarde, Data Protector lit les objets de sauvegarde, transfère leurs données via le réseau et les écrit sur les supports placés dans les périphériques.

> **IMPORTANT :**
> Assurez-vous que les données que vous sauvegardez sont cohérentes. Par exemple, vous pouvez fermer une application avant la sauvegarde ou la placer en mode "sauvegarde" afin d'éviter toute modification des données durant la sauvegarde. Si vous sauvegardez des données incohérentes, vous risquez d'obtenir des résultats inattendus lors de la restauration ou lorsque vous essaierez d'utiliser ces données.

Les fonctionnalités avancées de la sauvegarde Data Protector sont les suivantes :

- Équilibrage automatique de l'utilisation des périphériques (partage de charge)
- Sauvegarde des disques partagés
- Planification de sauvegardes sans surveillance
- Combinaison de sauvegardes complètes et incrémentales afin d'économiser du temps et des supports
- Possibilité d'organiser les sauvegardes de plusieurs façons
- Sauvegarde simultanée à plusieurs emplacements au moyen de la fonction de mise en miroir d'objets

Les procédures de l'aide Data Protector supposent que vous utilisez l'affichage de sauvegarde par défaut (Par type) qui est défini en fonction du type des données disponibles pour la sauvegarde ou le modèle.

Pour des informations sur la procédure de sauvegarde des applications de base de données telles qu'Oracle, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server, Informix Server, IBM DB2 UDB ou Sybase, reportez-vous au manuel *Guide d'intégration HPE Data Protector*.

Configuration de l'affichage de sauvegarde

Vous pouvez définir l'affichage de sauvegarde selon vos besoins. L'affichage de sauvegarde par défaut est Par type.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans le menu Affichage, sélectionnez celui qui vous convient.

Le contexte Sauvegarde s'affiche en fonction du choix que vous avez fait.

Types de sauvegarde

Data Protector propose deux types de sauvegarde de système de fichiers de base : complète et incrémentale. Ces types de sauvegarde s'appliquent à la spécification de sauvegarde complète et uniquement à des objets Système de fichiers.

Pour combiner des sauvegardes complètes et incrémentales, vérifiez que l'objet sauvegarde possède exactement les mêmes :

- nom de client
- lecteur/point de montage
- description
- propriétaire (pour les objets privés)

Si vous réalisez une sauvegarde interactive, vous êtes invité à sélectionner le type de sauvegarde. Lorsque vous planifiez une sauvegarde, vous spécifiez son type dans la boîte de dialogue assistantPlanifier la sauvegarde. Vous pouvez, par exemple, créer une planification pour exécuter la même spécification de sauvegarde de manière complète le samedi et incrémentale tous les jours ouvrables.

Sauvegardes complètes

Sauvegardes au cours desquelles tous les objets sélectionnés sont sauvegardés, même s'ils n'ont pas été modifiés depuis la sauvegarde précédente. La première sauvegarde d'un objet est toujours de type complète. Toute sauvegarde ultérieure sera réalisée de manière complète si aucune sauvegarde complète protégée avec le même propriétaire (pour les objets privés) n'existe lors de l'opération.

Sauvegardes incrémentales

Consistent à sauvegarder les modifications effectuées depuis une sauvegarde (complète ou incrémentale) précédente toujours protégée. La sauvegarde incrémentale d'un objet n'est possible que s'il existe une sauvegarde complète de ce dernier (avec un nom de client, un point de montage, une description et un propriétaire identiques).

Types de sauvegarde incrémentale

Data Protector propose différents types de sauvegarde incrémentale.

- Incr

  Une sauvegarde incrémentale simple est basée sur la dernière sauvegarde encore protégée, cette dernière pouvant être soit une sauvegarde complète soit une sauvegarde incrémentale.

- Incr1-9

  Une sauvegarde incrémentale par niveau dépend de la dernière sauvegarde en date du niveau immédiatement inférieur, dont les données sont toujours protégées. Par exemple, lors d'une sauvegarde Incr1, toutes les modifications effectuées depuis la dernière sauvegarde complète seront sauvegardées, alors que, lors d'une sauvegarde Incr5, seules les modifications effectuées

depuis la dernière sauvegarde Incr4 seront sauvegardées. Une sauvegarde Incr1-9 ne fait jamais référence à une sauvegarde Incr existante.

- Différentielle

  Terme utilisé dans certaines intégrations d'application pour une sauvegarde Incr1. Une sauvegarde différentielle enregistre toutes les modifications depuis la dernière sauvegarde complète.

Techniques de sauvegarde avancées

Data Protector fournit également des techniques de sauvegarde avancées, telles que la sauvegarde incrémentale avancée et la sauvegarde synthétique.

Sauvegardes complètes et incrémentales

Un moyen simple pour améliorer les performances de sauvegarde est de réduire le volume des données sauvegardées. Il est recommandé d'exploiter au mieux le temps et les ressources lors de la planification de vos sauvegardes complètes et incrémentales. La plupart du temps, il est inutile d'effectuer des sauvegardes complètes de tous les systèmes le même jour.

Avant de choisir le type de sauvegarde, nous vous recommandons de prendre en compte les points suivants :

	Sauvegarde complète	**Sauvegarde incrémentale**
Ressources	Prend plus de temps que la sauvegarde incrémentale et requiert davantage d'espace sur les supports.	Ne sauvegarde que les modifications apportées depuis la dernière sauvegarde, ce qui exige moins de temps et d'espace.
Gestion des supports	Si vous utilisez un périphérique autonome comportant un seul lecteur, vous devrez remplacer le support manuellement si l'intégralité du contenu de la sauvegarde ne tient pas sur un seul support.	Il est moins probable que la sauvegarde exige d'autres supports.
Restaurer	Permet une restauration simple et rapide.	La restauration prend plus de temps en raison du nombre de supports nécessaires.
Impact sur l'IDB	Occupe plus d'espace dans la Base de données interne (IDB).	Occupe moins d'espace dans la base de données interne.

REMARQUE :
Vous devez définir une protection des données appropriée pour garantir toutes les sauvegardes complètes et incrémentales nécessaires à la restauration. Si la protection des données n'est pas correctement définie, il est possible que la chaîne de restauration soit rompue.

Sauvegarde incrémentale classique

Comment fonctionne la sauvegarde incrémentale classique

Avant d'effectuer une sauvegarde incrémentale d'un objet sauvegarde, Data Protector compare les arborescences de l'objet sauvegarde à celles de la chaîne de restauration valide de l'objet en question. Si les arborescences ne concordent pas (par exemple, un répertoire supplémentaire de l'objet sauvegarde a été sélectionné pour la sauvegarde depuis la dernière sauvegarde ou il existe plusieurs spécifications de sauvegarde avec le même objet sauvegarde et des arborescences différentes), une sauvegarde complète est exécutée automatiquement. Ceci garantit que tous les fichiers sont inclus dans la sauvegarde.

Détection des modifications

Dans la sauvegarde incrémentale classique, c'est l'heure de modification du fichier qui permet de déterminer si ce dernier a été modifié ou non depuis la dernière sauvegarde. Toutefois, ce critère n'est pas efficace dans certains cas. Par exemple, si un fichier est renommé, déplacé, ou si certains de ses attributs sont modifiés, son heure de modification ne change pas. Dans ce cas, une sauvegarde incrémentale n'inclut pas toujours le fichier. De tels fichiers sont inclus dans la prochaine sauvegarde complète.

L'inclusion dans une sauvegarde incrémentale d'un fichier dont le nom, l'emplacement ou les attributs ont été modifiés dépend aussi de la valeur des options suivantes de la spécification de sauvegarde. L'option recommandée améliore la détection des modifications.

Systèmes Windows : Ne pas utiliser l'attribut archive

Par défaut, cette option n'est pas sélectionnée (l'attribut archive est utilisé). Il s'agit de l'option recommandée.

Systèmes UNIX : Ne pas conserver les attributs de temps d'accès

Par défaut, cette option n'est pas sélectionnée (les attributs de temps d'accès sont conservés). De préférence, cette option est sélectionnée.

Vous pouvez effectuer une sauvegarde incrémentale classique en utilisant le module fournisseur d'informations sur les modifications Windows NTFS. Dans ce cas, un Journal des modifications Windows est utilisé pour générer la liste des fichiers qui ont été modifiés depuis la dernière sauvegarde complète et aucun parcours de l'arborescence de fichiers n'est effectué. L'utilisation du module fournisseur d'informations sur les modifications améliore les performances globales des sauvegardes incrémentales de la même manière qu'elle améliore les performances des sauvegardes incrémentales avancées. Si le module fournisseur d'informations sur les modifications ne peut pas être utilisé pour quelque raison que ce soit, une sauvegarde incrémentale classique est effectuée.

Pour détecter et sauvegarder de manière fiable les fichiers renommés et déplacés, ainsi que ceux avec des modifications d'attributs, utilisez la sauvegarde incrémentale avancée.

Sauvegarde incrémentale avancée

Dans la sauvegarde incrémentale classique , c'est l'heure de modification du fichier qui permet de déterminer si ce dernier a été modifié ou non depuis la dernière sauvegarde. Toutefois, ce critère n'est pas efficace dans certains cas. Par exemple, si un fichier est renommé, déplacé, ou si certains de ses attributs sont modifiés, son heure de modification ne change pas. Dans ce cas, une sauvegarde incrémentale n'inclut pas toujours le fichier. De tels fichiers sont inclus dans la prochaine sauvegarde complète.

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

La détection de certaines modifications (par exemple, en matière d'autorisations ou de listes de contrôle d'accès) dépend aussi de la valeur des options suivantes de la spécification de sauvegarde. La valeur recommandée améliore la détection des modifications pour la sauvegarde incrémentale avancée.

- **Systèmes Windows :** Ne pas utiliser l'attribut archive

  Par défaut, cette option n'est pas sélectionnée (l'attribut archive est utilisé). Il s'agit de l'option recommandée.
- **Systèmes UNIX :** Ne pas conserver les attributs de temps d'accès

  Par défaut, cette option n'est pas sélectionnée (les attributs de temps d'accès sont conservés). La sélection de cette option est recommandée.

Ce type de sauvegarde permet également d'éviter les sauvegardes complètes inutiles d'un objet sauvegarde dans son intégralité lorsque certaines des arborescences sélectionnées pour la sauvegarde changent. Par exemple, si vous sélectionnez un autre répertoire pour la sauvegarde depuis la dernière effectuée, une sauvegarde complète de ce répertoire (arborescence) est réalisée, le reste faisant l'objet d'une sauvegarde incrémentale.

Vous pouvez également effectuer des sauvegardes incrémentales avancées en utilisant le module fournisseur d'informations sur les modifications Windows NTFS. Dans ce cas, un Journal des modifications Windows est utilisé pour générer la liste des fichiers qui ont été modifiés depuis la dernière sauvegarde complète et aucun parcours de l'arborescence de fichiers n'est effectué. Le module fournisseur d'informations sur les modifications augmente les performances globales de la sauvegarde incrémentale, en particulier dans les environnements qui contiennent des millions de fichiers, dont quelques-uns seulement ont été modifiés.

Avantages de l'utilisation de la sauvegarde incrémentale avancée

Utilisez la sauvegarde incrémentale avancée pour :

- Assurer une sauvegarde incrémentale des fichiers dont le nom, l'emplacement ou les attributs sont modifiés.
- Eliminer les sauvegardes complètes inutiles en cas de modification de certaines arborescences sélectionnées.
- Activer une consolidation d'objets ultérieure (sauvegarde synthétique).

Impact sur l'utilisation de l'espace disque

La sauvegarde incrémentale avancée utilise une petite base de données sur chaque client sauvegardé. La base de données est créée pour chaque point de montage du système de fichiers. Le référentiel de sauvegarde incrémentale avancée est situé dans le répertoire suivant :

- **Systèmes Windows :** *répertoire_Data_Protector*\enhincrdb*MountPointDir*

  Le répertoire de point de montage (MountPointDir) est obtenu à partir du nom du point de montage en remplaçant tous les caractères ":" (deux-points) and "\" (barre oblique inversée) par les caractères "_" (trait de soulignement) et en enlevant le ":" ou le "\". final.
- **Systèmes HP-UX et Linux :** /var/opt/omni/enhincrdb

L'impact sur l'espace disque du client est en général inférieur à 1 % de la taille des fichiers sélectionnés pour la sauvegarde. Veillez à purger régulièrement la base de données de sauvegarde incrémentale avancée. Pour ce faire, il suffit de définir les options omnirc OB2_ENHINC_DELETE_INTERVAL et OB2_ENHINC_DELETE_THRESHOLD.

Agents de disque simultanés

Plusieurs Agents de disque peuvent accéder simultanément à la base de données de sauvegarde incrémentale avancée. Pour éviter tout problème avec la sauvegarde, configurez le comportement des Agents de disque en définissant les options omnirc suivantes :

- OB2_ENHINC_LOCK_TIMEOUT
- OB2_ENHINC_SQLITE_MAX_ROWS
- OB2_ENHINC_MAX_MEMORY_LIMIT

Limites

- La sauvegarde incrémentale avancée est seulement prise en charge au niveau d'un répertoire. Si vous sélectionnez des fichiers individuels à sauvegarder, ce mode de sauvegarde n'est pas utilisé.
- La détection des liaisons permanentes est désactivées lorsque le mode incrémental amélioré est utilisé.

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

Avec une sauvegarde incrémentale avancée ou conventionnelle, une liste de fichiers à sauvegarder est générée en effectuant un parcours de l'arborescence de fichiers. Ce processus peut prendre un temps considérable, en particulier quand la structure de répertoires est de grande taille et contient des millions de fichiers. Le module fournisseur d'informations sur les modifications Windows NTFS, fondé sur le Journal des modifications de Windows, permet de résoudre ce problème en interrogeant le Journal des modifications pour obtenir la liste des fichiers modifiés, au lieu de procéder à un parcours de l'arborescence de fichiers. En toute fiabilité, le Journal des modifications détecte et consigne toutes les modifications apportées aux fichiers et répertoires d'un volume NTFS, ce qui permet à Data Protector de se servir de ce journal en tant que mécanisme de suivi afin de générer la liste des fichiers qui ont été modifiés depuis la dernière sauvegarde complète. Ceci s'avère très avantageux dans les environnements comportant des systèmes de fichiers de très grande taille, dans lesquels seul un

pourcentage minime de fichiers est modifié entre les sauvegardes. Dans ce cas, le processus de détermination des fichiers modifiés s'effectue sous un délai bien plus court.

Chaque volume NTFS comporte sa propre base de données de Journal des modifications. Dès qu'une modification est apportée à un fichier ou à un répertoire, un enregistrement est ajouté en fin de journal. L'enregistrement identifie le nom de fichier, l'heure et le type de modification. Notez que les données modifiées réelles ne sont pas conservées dans le journal. Si le fichier journal devient trop volumineux, le système purge les enregistrements les plus anciens, qui figurent au début. Si les données requises pour la sauvegarde ont été purgées dans le Journal des modifications, Data Protector procède à une sauvegarde complète et renvoie un avertissement indiquant que le Journal des modifications n'a pas pu être utilisé.

Un fichier est sauvegardé ou non dans une sauvegarde incrémentale utilisant le fournisseur d'informations sur les modifications en fonction de l'option Utiliser le module fournisseur d'informations sur les modifications du système de fichiers natif s'il est disponible dans une spécification de sauvegarde. Si cette option a été spécifiée, Data Protector tente d'utiliser le Journal des modifications. Si le Journal des modifications n'est pas actif, Data Protector émet un avertissement. Si cela se produit pendant la sauvegarde incrémentale avancée, une sauvegarde complète est effectuée à la place. Si cela se produit pendant la sauvegarde incrémentale classique, une sauvegarde incrémentale normale est effectuée à la place. Les options Ne pas préserver les attributs de temps d'accès et Ne pas utiliser l'attribut archive sont configurées automatiquement et ne peuvent pas être désactivées.

Conditions préalables

- Assurez-vous que le Journal des modifications est activé sur un volume au moyen de la commande `omnicjutil -query`. Si le Journal des modifications n'est pas actif, exécutez `omnicjutil -start`. Pour plus d'informations sur la commande `omnicjutil`, voir *Guide de référence de l'interface de ligne de commande HPE Data Protector* situé dans le package d'installation qui se trouve dans ce répertoire *`Mount_point`*`/DOCS/C/MAN`.
- Assurez-vous qu'il existe au moins une sauvegarde complète (option **Utiliser le module fournisseur d'informations sur les modifications du système de fichiers natif s'il est disponible** sélectionnée dans la spécification de sauvegarde) avant de lancer une sauvegarde incrémentale avancée au moyen du module fournisseur d'informations sur les modifications.

Performances et occupation de l'espace disque

Pour obtenir les meilleures performances possible avec le module fournisseur d'informations, utilisez des sauvegardes incrémentales lorsque vous lancez la sauvegarde (le type de sauvegarde est Incr). Incr1-9 est également pris en charge, mais au risque de dégradations des performances.

Lorsqu'il est activé, le Journal des modifications consomme du temps processeur et de l'espace disque. La consommation d'espace disque est limitée à 4 Go. Vous pouvez définir la taille maximale du Journal des modifications, ainsi que la taille à laquelle le journal doit être tronqué quand il atteint sa taille maximale. Pour plus d'informations, voir *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Pour optimiser les performances du module fournisseur d'informations sur les modifications, vous pouvez indiquer le nombre d'entrées qu'il peut conserver en mémoire au moyen de la variable omnirc `OB2_CLP_MAX_ENTRIES`. Pour plus d'informations, reportez-vous à la section *Guide de dépannage HPE Data Protector*.

Dans les cas suivants, Data Protector effectue une sauvegarde complète et ignore la définition du fournisseur d'informations sur les modifications figurant dans une spécification de sauvegarde :

- si le Journal des modifications n'est pas actif sur le système client ;
- si les données souhaitées ont été purgées du Journal des modifications ;
- si l'ID du Journal des modifications a changé (lorsqu'une autre application a supprimé, puis recréé le journal).

Par défaut, le module fournisseur d'informations sur les modifications ne crée pas le référentiel incrémental avancé au moment de sa première exécution. A la première erreur du fournisseur d'informations sur les modifications, une sauvegarde complète est effectuée et le référentiel incrémental avancé est créé. Ce comportement peut être modifié avec l'option omnirc `OB2_CLP_CREATE_EI_REPOSITORY`. Pour plus d'informations, consultez le *Guide de dépannage HPE Data Protector*.

Points à prendre en considération

- Data Protector ne dispose pas d'un accès exclusif au Journal des modifications. Cela signifie que lorsque vous activez ou désactivez le Journal des modifications, d'autres applications peuvent agir sur Data Protector. Si un Journal des modifications est désactivé sur un volume donné, aucune modification de fichier et de répertoire n'est consignée. Par défaut, le Journal des modifications d'un volume NTFS est désactivé, vous devez donc l'activer explicitement avec la commande `cjutil` ou `omnicjutil`. D'un autre côté, n'importe quelle autre application peut activer ou désactiver le journal du volume à tout moment. Pour plus d'informations sur le Journal des modifications, consultez la documentation Windows.

  Notez que sous Windows Vista, Windows 7, Windows 8, Windows Server 2008, et Windows Server 2012, le Journal des modifications est activé par défaut.
- Le module fournisseur d'informations sur les modifications est particulièrement utile dans les environnements où peu de modifications sont apportées au système de fichiers. La sauvegarde d'un système de fichiers avec un grand nombre de modifications (par exemple, de nombreux fichiers temporaires créés puis supprimés peu après) est plus rapide avec un parcours d'arborescence normal.
- L'API du Journal des modifications Windows ne fournit aucune information détaillée sur les attributs. Tous les changements d'attributs sont regroupés. L'API ne permet pas de déterminer si une entrée du Journal des modifications a pour origine la désactivation d'un attribut archive ou une modification apportée lors du dernier accès.

  Le module fournisseur d'informations sur les modifications ne désactive pas l'attribut archive. Par défaut, Data Protector désactive l'attribut archive après que le fichier a été sauvegardé. C'est pourquoi lorsque le module fournisseur d'informations sur les modifications est actif, l'option **Ne pas utiliser l'attribut archive** est sélectionnée automatiquement.

  Par défaut, Data Protector réinitialise l'heure du dernier accès après que le fichier a été sauvegardé (car le processus de sauvegarde modifie toujours l'heure du dernier accès). Le module fournisseur d'informations ne la réinitialise pas, et l'option **Ne pas conserver les attributs de temps d'accès** est donc sélectionnée automatiquement.

  Ces deux options sont sélectionnées automatiquement afin d'éviter des situations où les mêmes fichiers sont sauvegardés plusieurs fois. Si l'attribut archive est désactivé ou si l'heure du dernier accès est réinitialisée, une entrée figure dans le Journal des modifications et les fichiers sont sauvegardés lors la session suivante, même s'ils n'ont pas été modifiés.

- Surveillez de temps à autre la valeur `NextUsn` à l'aide de la commande `cjutil - query` et redémarrez le Journal des modifications quand `NextUsn` s'approche de la valeur `MaxUsn`.
- Si une spécification de sauvegarde a été modifiée, toutes les nouvelles arborescences sont entièrement sauvegardées. Cela signifie qu'un parcours d'arborescence normal est effectué sur toutes les nouvelles arborescences et que le module fournisseur d'informations sur les modifications est utilisé sur les anciennes.
- Si un répertoire situé sous l'espace de sauvegarde est renommé, un parcours d'arborescence normal est effectué sur ce répertoire.

Limites

- Seule la sauvegarde de volumes NTFS Windows est supportée.

Sauvegarde synthétique

La sauvegarde synthétique est une solution de sauvegarde avancée qui évite d'avoir à lancer régulièrement des sauvegardes complètes. Après une sauvegarde complète initiale, seules des sauvegardes incrémentales sont réalisées, puis fusionnées avec la sauvegarde complète en une nouvelle sauvegarde complète synthétique. Ce processus peut se répéter indéfiniment, sans besoin d'exécuter une autre sauvegarde complète. En termes de vitesse de restauration, une telle sauvegarde est équivalente à une sauvegarde complète classique.

Data Protector exécute une sauvegarde synthétique au moyen d'une opération appelée consolidation d'objets.

Exécution d'une sauvegarde synthétique

La procédure de sauvegarde synthétique est la suivante :

1. Dans la spécification de sauvegarde utilisée pour la sauvegarde complète et les sauvegardes incrémentales, activez l'option **Sauvegarde incrémentielle avancée**.
2. Réalisez une sauvegarde complète.
3. Configurez l'écriture des sauvegardes incrémentales suivantes dans une bibliothèque de fichiers ou des périphériques B2D (à l'exception de Smart Cache).
4. Lorsqu'au moins une sauvegarde incrémentale existe, effectuez une consolidation d'objet. La fréquence de la consolidation d'objet dépend de votre stratégie de sauvegarde.

Sauvegarde complète virtuelle

La sauvegarde complète virtuelle est une variante optimisée de la sauvegarde synthétique. Cette technique utilise des pointeurs pour consolider les données au lieu de les copier. L'opération prend ainsi moins de temps et évite une duplication inutile des données.

La procédure est fondamentalement identique à celle d'une sauvegarde synthétique normale, avec en outre les exigences suivantes :

- Il faut effectuer l'écriture de toutes les sauvegardes dans une bibliothèque de fichiers : la sauvegarde complète, les sauvegardes incrémentales et la sauvegarde complète virtuelle résultante.

- La bibliothèque de fichiers doit utiliser le format de support de fichiers distribués.

> **REMARQUE :**
> La sauvegarde complète virtuelle permet de réduire l'utilisation d'espace, car les objets partagent les mêmes blocs de données. Toutefois, en cas d'altération d'un bloc de données, plusieurs objets peuvent être affectés. Pour une fiabilité optimale, gardez la bibliothèque de fichiers sur un disque RAID.

Procédure de sauvegarde standard

La procédure de sauvegarde standard se déroule en plusieurs étapes :

- sélection des données à sauvegarder,
- sélection de la destination de la sauvegarde,
- sélection du nombre de copies de sauvegarde supplémentaires (miroirs) à créer,
- démarrage ou planification d'une session de sauvegarde.

Ceci est effectué en créant une spécification de sauvegarde. Différentes options permettent de définir la façon dont la sauvegarde est effectuée. Vous pouvez soit utiliser les valeurs par défaut, soit les adapter à vos besoins spécifiques.

Pour changer les paramètres prédéfinis, spécifiez les éléments suivants :

- les options de sauvegarde pour tous les objets dans la spécification de sauvegarde cible telles que pré-exécution et protection des données
- les dates et heures auxquelles les sauvegardes doivent être effectuées.

Conditions préalables

- Un Agent de disque doit être installé sur chaque système à sauvegarder, à moins que vous n'utilisiez NFS (sur les systèmes UNIX) ou que vous n'effectuiez une sauvegarde partagée sur le réseau (sur les systèmes Windows) pour sauvegarder ces systèmes.
- Vous devez également avoir au moins un périphérique de sauvegarde configuré dans la cellule Data Protector.
- Les supports doivent avoir été préparés pour la sauvegarde.
- Vous devez avoir les droits utilisateur pour effectuer une sauvegarde.

Sauvegarde de système de fichiers

Pour chaque système de fichiers, vous pouvez limiter la sauvegarde à certaines arborescences de répertoires. Pour chaque arborescence, vous pouvez :

- exclure tout répertoire ou fichier ;
- sauvegarder les fichiers correspondant à un modèle de recherche donné ;
- ignorer les fichiers correspondant à un modèle de recherche donné.

Certains fichiers sont utilisés en permanence. par exemple par des applications logicielles. Vous devez exclure ces fichiers d'une sauvegarde de système de fichiers et les sauvegarder de manière spéciale.

Création d'une spécification de sauvegarde

La spécification de sauvegarde définit les clients, les disques, les répertoires et les fichiers à sauvegarder. Elle définit également les périphériques ou les lecteurs à utiliser, le nombre de copies de sauvegarde supplémentaires (miroirs), les options de sauvegarde et fournit des informations de programmation (date et heure des sauvegardes). Elle peut être très simple (sauvegarde d'un disque sur un lecteur DDS autonome) ou très complexe (sauvegarde de 40 serveurs volumineux sur une bibliothèque à bande comportant huit lecteurs).

Limitations

- L'interface utilisateur graphique de Data Protector permet d'afficher un nombre limité de spécifications de sauvegarde. Le nombre de spécifications de sauvegarde dépend de la taille de leurs paramètres (informations sur le nom, le groupe, la propriété et le partage de charge). Cette taille ne doit pas dépasser 80 Ko.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**.
3. Cliquez avec le bouton droit de la souris sur l'élément à sauvegarder (par exemple, **Système de fichiers**), puis sélectionnez **Ajouter sauvegarde**.
4. Dans la boîte de dialogue **Créer sauvegarde**, sélectionnez l'un des modèles disponibles, le type de sauvegarde et paramétrez éventuellement d'autres options. Cliquez sur **OK** pour ouvrir l'assistant.
5. Dans le cas d'une sauvegarde avec temps d'indisponibilité nul, la page Configuration s'affiche. Configurez l'intégration et cliquez sur **Suivant**.
6. Dans le cas d'une sauvegarde d'intégration, sélectionnez le client et la base de données de l'application. Cliquez sur **Suivant**.
7. Dans la page de propriétés Source, développez le système contenant les objets à sauvegarder, puis sélectionnez ce que vous souhaitez sauvegarder.

   > **IMPORTANT :**
   > Sur les systèmes UNIX, si vous envisagez d'exécuter une restauration instantanée, sélectionnez tous les systèmes de fichiers du groupe de volumes à sauvegarder. Sinon, la restauration instantanée via l'interface utilisateur graphique de Data Protector sera impossible ou (si vous utilisez l'interface de ligne de commande de Data Protector pour la restauration instantanée) les données risquent d'être endommagées.

   Cliquez sur **Suivant**.
8. Dans la page de propriétés Destination, sélectionnez le(s) périphérique(s) à utiliser pour la sauvegarde.

   Vous pouvez également indiquer si vous souhaitez créer des copies supplémentaires (miroirs) de votre sauvegarde au cours de la session de sauvegarde. Indiquez le nombre de miroirs souhaité en cliquant sur les boutons **Ajouter miroir** et **Supprimer miroir**. Sélectionnez des périphériques

distincts pour la sauvegarde et pour chaque miroir. Il n'est pas possible de mettre en miroir des objets sauvegardés à l'aide de ZDB sur disque ou NDMP.

> **CONSEIL :**
> Si la sauvegarde est en partage de charge, vous pouvez définir l'ordre dans lequel Data Protector utilisera les périphériques en cliquant avec le bouton droit sur un périphérique sélectionné, puis en cliquant sur **Trier périphériques**.

Cliquez sur **Suivant**.

9. Dans la page de propriétés Options, vous pouvez définir les options de sauvegarde. Les options disponibles varient en fonction du type de données sauvegardées. Par exemple, vous ne disposerez pas des mêmes options de sauvegarde pour la sauvegarde d'un système de fichiers et celle d'une image disque. Cliquez sur **Suivant**.
10. Dans la page Résumé de sauvegarde, consultez le résumé de la spécification de sauvegarde. Il est recommandé de commencer par enregistrer la spécification de sauvegarde, puis de lancer un test. Il n'y a pas de test disponible pour la sauvegarde de base de données interne Data Protector les sessions de sauvegarde d'intégrations spécifiques d'applications Data Protector et la sauvegarde avec temps d'indisponibilité nul (ZDB). Cliquez sur **Suivant**.
11. À la fin de l'assistant de sauvegarde, vous pouvez enregistrer, enregistrer et planifier, démarrer ou tester la sauvegarde configurée. Il se passe alors ce qui suit :
    - Si vous enregistrez la sauvegarde configurée, celle-ci s'affiche dans le contexte Sauvegarde de la fenêtre de navigation sous la forme d'une nouvelle spécification de sauvegarde. Par la suite, vous pouvez la tester ou la lancer telle quelle, ou la modifier, puis la tester ou la lancer.
    - Si vous avez enregistré et planifié la sauvegarde configurée, la spécification de sauvegarde est d'abord enregistrée, puis la page Planificateur s'ouvre pour vous permettre de spécifier les dates et heures auxquelles cette spécification de sauvegarde enregistrée doit s'exécuter.
    - Si vous démarrez ou testez la sauvegarde configurée, le message Informations de session affiche l'état de la sauvegarde.

> **CONSEIL :**
> Vous pouvez créer plusieurs spécifications de sauvegarde en copiant une spécification existante, puis en modifiant l'une des copies.

Modification d'une spécification de sauvegarde

Vous pouvez modifier une spécification de sauvegarde déjà configurée et enregistrée.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécifications de sauvegarde**, puis développez le type de spécifications de sauvegarde approprié (par exemple **Système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez sur la spécification de sauvegarde à modifier.

4. Dans la page de propriétés Source, ainsi que dans les autres pages de propriétés (Destination, Options et Planifier), modifiez la spécification de sauvegarde, puis cliquez sur Appliquer.

Une fois que vous avez modifié votre sauvegarde, vous pouvez la tester ou la démarrer dans le menu Actions.

> **REMARQUE :**
> Il n'y a pas de test disponible pour la sauvegarde de base de données interne Data Protector les sessions de sauvegarde d'intégrations spécifiques d'applications Data Protector et la sauvegarde avec temps d'indisponibilité nul (ZDB).

> **CONSEIL :**
> Lorsque vous modifiez une spécification de sauvegarde, effectuez la sauvegarde puis sélectionnez l'objet à restaurer : seuls les fichiers et les répertoires sauvegardés dans la dernière version sont sélectionnés pour la restauration. Pour changer la version de sauvegarde, cliquez sur l'objet avec le bouton droit, puis cliquez sur **Sélectionner version**.

Test et démarrage d'une sauvegarde

Vous pouvez tester une sauvegarde afin de vérifier vos choix. Au cours de cette opération, les données sélectionnées pour la sauvegarde ne sont ni lues sur les disques ni écrites sur les supports du périphérique configuré. Le logiciel se contente de vérifier que les communications au sein de l'infrastructure utilisée fonctionnent correctement et de déterminer la taille des données ainsi que la disponibilité des supports cibles.

Vous pouvez démarrer une sauvegarde (configurée et enregistrée) existante après avoir fourni à Data Protector toutes les informations nécessaires.

Limites

- Le test n'est pas disponible pour la sauvegarde de base de données Data Protector et les sessions de sauvegarde d'intégrations d'application Data Protector spécifiques.
- Le test n'est pas disponible pour la sauvegarde avec temps d'indisponibilité nul (ZDB).

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**, puis le type de spécification approprié (par exemple **système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Sélectionnez la spécification de sauvegarde à démarrer ou à tester.
4. Dans le menu **Actions**, cliquez sur **Tester sauvegarde** si vous souhaitez la tester ou sur **Démarrer sauvegarde** pour la lancer.
5. Dans la boîte de dialogue Tester ou Démarrer sauvegarde, sélectionnez le type de sauvegarde (complète ou incrémentale ; d'autres types de sauvegarde sont disponibles pour certaines intégrations) et la charge réseau.

Dans le cas de ZDB sur disque + bande ou ZDB sur disque (la restauration instantanée est activée), spécifiez l'option Sauvegarde Split Mirror/Snapshot.

6. Cliquez sur **OK** pour tester ou démarrer la sauvegarde.

Le message Informations de session affiche l'état de la sauvegarde.

> **CONSEIL :**
> Lorsque vous configurez une nouvelle sauvegarde, démarrez une sauvegarde interactive ou un test interactif à la fin de la procédure proposée par l'assistant.

Abandon d'une sauvegarde

L'abandon d'une session de sauvegarde termine une session de sauvegarde. Seules les données qui ont été sauvegardées avant l'abandon de la session font l'objet d'une copie de sauvegarde.

Procédure

1. Dans le menu Actions, cliquez sur Abandonner pour abandonner une session de sauvegarde.

   Si vous abandonnez une session de sauvegarde alors que le logiciel est encore en train de déterminer la taille des disques que vous avez sélectionnés, la sauvegarde n'est pas abandonnée immédiatement. L'opération s'effectue une fois que les tailles des disques ont été déterminées.

> **CONSEIL :**
> Vous pouvez abandonner une ou plusieurs sessions en cours dans le contexte Moniteur Data Protector.

Redémarrage des sauvegardes ayant échoué

Lors d'une session de sauvegarde, il est possible que certains systèmes ne soient pas disponibles car ils sont éteints, parce qu'il existe des problèmes temporaires de connectivité réseau, etc. Par conséquent, certains systèmes peuvent ne pas être sauvegardés ou n'être sauvegardés que partiellement. En d'autres mots, certains objets ont échoué. Vous pouvez relancer une session avec des erreurs après avoir résolu les problèmes imminents. Cette action ne redémarre que les objets ayant échoué.

Conditions préalables

- Vous devez être membre du groupe d'utilisateurs Admin Data Protector ou disposer des droits utilisateur Moniteur Data Protector.

Points à prendre en considération

- Pour les sessions de sauvegarde de l'intégration avec Oracle Server et de système de fichiers ayant échoué, vous pouvez aussi utiliser la fonction de reprise de session pour continuer la sauvegarde à partir de l'endroit où la session a échoué.

Limites

- Vous ne pouvez pas redémarrer des sessions ayant échoué après avoir été exécutées de façon interactive, ce qui signifie qu'elles reposent sur des spécifications de sauvegarde non enregistrées.
- Il n'est pas possible de redémarrer plusieurs sessions simultanément.

> **IMPORTANT :**
> Ne modifiez pas une spécification de sauvegarde avant de redémarrer une session de sauvegarde ayant échoué. En effet, il ne serait pas possible de redémarrer tous les objets.

Procédure

1. Si vous utilisez un Gestionnaire de cellule ordinaire, cliquez sur **Base de données interne** dans la liste de contexte.

   Si vous utilisez un Manager-of-Managers, choisissez **Clients** dans la liste de contexte, puis développez **Clients d'entreprise**. Sélectionnez un Gestionnaire de cellule rencontrant un problème de session. Dans le menu Outils, sélectionnez **Administration base de données** pour ouvrir une nouvelle fenêtre d'interface utilisateur Data Protector dans laquelle apparaît le contexte de la base de données interne.
2. Dans la fenêtre de navigation, développez **Base de données interne**, puis cliquez sur **Sessions**.

   Une liste de sessions s'affiche dans la zone de résultats. L'état de chaque session est indiqué dans la colonne Etat.
3. Cliquez avec le bouton droit de la souris sur une session ayant échouée, abandonnée, ou encore une session s'étant achevée avec des échecs ou des erreurs, puis sélectionnez **Redémarrer objets ayant échoué** pour sauvegarder les objets ayant échoué.
4. Cliquez sur **Oui** pour confirmer.

Copie d'une spécification de sauvegarde

Vous pouvez copier une spécification de sauvegarde déjà configurée et enregistrée.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécifications de sauvegarde**, puis développez le type de spécifications de sauvegarde approprié (par exemple **Système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Dans la zone de résultats, cliquez avec le bouton droit sur la spécification de sauvegarde à copier, puis cliquez sur **Copier sous**. La boîte de dialogue Copier sauvegarde sous s'affiche.
4. Dans la zone de texte Nom, attribuez un nom à la spécification de sauvegarde copiée. Le cas échéant, dans la liste déroulante Groupe, sélectionnez le groupe de spécifications de sauvegarde auquel la spécification de sauvegarde copiée doit appartenir.
5. Cliquez sur **OK**.

La spécification de sauvegarde copiée s'affiche dans le contexte Sauvegarde dans la fenêtre de navigation ainsi que dans la zone de résultats sous son nouveau nom.

Suppression d'une spécification de sauvegarde

Vous pouvez supprimer une spécification de sauvegarde déjà configurée et enregistrée.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez Spécifications de sauvegarde, puis développez le type de spécifications de sauvegarde approprié (par exemple Système de fichiers). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez avec le bouton droit sur la spécification de sauvegarde à supprimer, puis cliquez sur Supprimer. Confirmez ensuite votre choix.

La spécification de sauvegarde est supprimée du contexte Sauvegarde de la fenêtre de navigation.

Tâches de sauvegarde avancées

Il est possible de contrôler une sauvegarde de plusieurs façons. Data Protector propose un ensemble de tâches de sauvegarde avancées pour les systèmes Windows et UNIX.

Conditions préalables

- Un Agent de disque doit être installé sur chaque système à sauvegarder, à moins que vous n'utilisiez NFS (sur les systèmes UNIX) ou que vous n'effectuiez une sauvegarde partagée sur le réseau (sur les systèmes Windows) pour sauvegarder ces systèmes.
- Vous devez également avoir au moins un périphérique de sauvegarde configuré dans la cellule.
- Les supports doivent avoir été préparés pour la sauvegarde.
- Vous devez avoir les droits utilisateur pour effectuer une sauvegarde.
- Enfin, avant de poursuivre, vous devez prendre connaissance de la procédure de sauvegarde standard.

Qu'est-ce qu'une tâche de sauvegarde avancée ?

Il s'agit de la spécification d'options non définies par défaut ou d'une action ne suivant pas la procédure de sauvegarde standard.

- Sélection d'un disque partagé du réseau pour la sauvegarde
- Sélection de certains fichiers (correspondant à une recherche) à sauvegarder
- Fichiers ignorés lors de la sauvegarde
- Sélection de l'emplacement du raccourci pour le démarrage d'une sauvegarde
- Sauvegarde à l'aide de plusieurs Agents de disque
- Sauvegarde d'un client avec découverte des disques

- Sauvegarde d'image de disque
- Sauvegarde d'un serveur Web

Sélection d'un disque partagé du réseau pour la sauvegarde

Vous pouvez sauvegarder les données sur des disques partagés Windows. Vous devez utiliser un client Agent de disque Data Protector standard pour sauvegarder d'autres systèmes distants via des disques partagés.

La méthode de sauvegarde sur disque partagé est une solution alternative permettant de sauvegarder des systèmes qui ne peuvent pas être sauvegardés autrement. Cette méthode ne devrait pas être utilisée comme principale solution de sauvegarde.

Sauvegarde d'un système de fichiers situé sur un système Windows partagé sur le réseau :

- Si le système ne fait pas partie de la cellule Data Protector et ne dispose pas de l'Agent de disque Data Protector.
- Vous souhaitez effectuer des sauvegardes vers des plates-formes qui ne sont pas directement prises en charge par Data Protector, telles que les systèmes Windows pour Workgroups, Windows 3.1 ou Windows NT.

> **CONSEIL :**
> Pour réduire la charge réseau, un client Agent de disque devrait également servir de client Agent de support. Sinon, les données sont transférées deux fois sur le réseau.

Conditions préalables

Vous devez modifier le compte Inet Data Protector sur le client Agent de disque afin de disposer des autorisations appropriées pour accéder au disque partagé vers lequel vous souhaitez effectuer la sauvegarde. Une autorisation d'accès au système client local et aux disques partagés distants doit être associée à ce compte. Pour les versions Windows antérieures à Windows Vista et à Windows Server 2008, le compte doit être un compte utilisateur spécifique et non pas le compte système local.

Une fois que vous avez configuré le compte utilisateur pour le service Inet, vous pouvez sauvegarder les disques partagés comme s'ils résidaient sur le système local.

Windows Vista, Windows 7, Windows 8, Windows Server 2008 et Windows Server 2012

Vous devez ajouter un compte utilisateur autorisé à accéder au disque partagé que vous voulez sauvegarder. Ce compte doit être un compte système local.

Ces conditions préalables doivent être remplies avant de modifier le compte Inlet Data Protector sur le client Agent de disque. Exécutez la commande suivante sur le client Data Protector sur lequel l'Agent de disque sera exécuté :

```
omniinetpasswd -add User@Domain [Password]
```

Conditions préalables

- Vous devez mapper les disques partagés en utilisant l'assistant de sauvegarde.
- Utilisez l'interface graphique Windows car la navigation des systèmes Windows n'est pas prise en charge dans l'interface graphique UNIX.

Limites

- La sauvegarde de disques partagés ne sauvegarde pas tous les attributs de fichier. Seuls les éléments visibles sur le partage hôte peuvent être sauvegardés. Les données peuvent être restaurées, mais certains attributs de fichier/répertoire peuvent être manquants.
- La sauvegarde de modules d'écriture stockant leurs données sur des volumes réseau partagés à l'aide de la fonctionnalité VSS n'est pas prise en charge. De même, la sauvegarde de partages réseau ou de dossiers réseau distants avec un Agent de disque et l'option Utiliser Shadow Copy activée n'est pas prise en charge sur Windows Server 2012.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**.
3. Cliquez avec le bouton droit de la souris sur l'élément à sauvegarder (par exemple, **Système de fichiers**), puis sélectionnez **Ajouter sauvegarde**.
4. Dans la boîte de dialogue **Créer sauvegarde**, sélectionnez l'un des modèles disponibles, puis cliquez sur **OK** pour lancer l'assistant.
5. Dans la page de propriétés Source, sélectionnez **Sauvegarde de partage réseau** dans la liste déroulante (disponible si l'interface graphique s'exécute sur des systèmes Windows).
6. Cliquez sur **Mapper partage réseau** pour ouvrir la fenêtre **Explorer les partages réseau**.
7. Dans la liste déroulante Système client, sélectionnez le système client possédant l'Agent de disque à utiliser pour la sauvegarde.
8. Dans la zone Répertoires partagés, sélectionnez ou spécifiez le disque partagé, puis cliquez sur **OK**. Si vous souhaitez sélectionner plusieurs disques, cliquez sur **Appliquer**.
9. Dans la page de propriétés Source, sélectionnez ou spécifiez les systèmes de fichiers partagés à sauvegarder. Cliquez sur **Suivant**.
10. Dans la page de propriétés Destination, sélectionnez le(s) périphérique(s) à utiliser pour la sauvegarde.

    Vous pouvez également indiquer si vous souhaitez créer des copies supplémentaires (miroirs) de votre sauvegarde au cours de la session de sauvegarde. Indiquez le nombre de miroirs souhaité en cliquant sur les boutons **Ajouter miroir** et **Supprimer miroir**. Sélectionnez des périphériques distincts pour la sauvegarde et pour chaque miroir. Il n'est pas possible de mettre en miroir des objets sauvegardés à l'aide de la fonction de sauvegarde ZDB sur disque ou NDMP.

    > **CONSEIL :**
    > Si la sauvegarde est en partage de charge, vous pouvez définir l'ordre dans lequel Data

> Protector utilisera les périphériques en cliquant avec le bouton droit sur un périphérique sélectionné, puis en cliquant sur **Trier périphériques**.

Cliquez sur **Suivant**.

11. Dans la page de propriétés Options, vous pouvez définir les options de sauvegarde. Les options disponibles varient en fonction du type de données sauvegardées. Par exemple, vous ne disposerez pas des mêmes options de sauvegarde pour la sauvegarde d'un système de fichiers et celle d'une image disque.

    Sous Windows Vista, Windows 7, Windows 8, Windows Server 2008 et Windows Server 2012, procédez comme suit :

    a. Sous Options de spécification de sauvegarde, cliquez sur le bouton **Avancé**.
    b. Dans la boîte de dialogue Options de sauvegarde, sous Propriété, entrez les informations concernant le compte utilisateur autorisé à accéder au disque partagé qui sera sauvegardé.
    c. Cliquez sur **OK**.
12. Cliquez sur **Suivant**.
13. Dans la page Résumé de sauvegarde, consultez le résumé de la spécification de sauvegarde. Il est recommandé de commencer par enregistrer la spécification de sauvegarde, puis de lancer un test. Cliquez sur **Suivant**.
14. À la fin de l'assistant de sauvegarde, vous pouvez enregistrer, enregistrer et planifier, démarrer ou tester la sauvegarde configurée. Il se passe alors ce qui suit :
    - Si vous enregistrez la sauvegarde configurée, celle-ci s'affiche dans le contexte Sauvegarde de la fenêtre de navigation sous la forme d'une nouvelle spécification de sauvegarde. Par la suite, vous pouvez la tester ou la lancer telle quelle, ou la modifier, puis la tester ou la lancer.
    - Si vous avez enregistré et planifié la sauvegarde configurée, la spécification de sauvegarde est d'abord enregistrée, puis la page Planificateur s'ouvre pour vous permettre de spécifier les dates et heures auxquelles cette spécification de sauvegarde enregistrée doit s'exécuter.
    - Si vous démarrez ou testez la sauvegarde configurée, le message Informations de session affiche l'état de la sauvegarde.

Un Agent de disque est lancé pour chaque disque que vous sauvegardez. Les performances de votre sauvegarde peuvent diminuer si vous lancez trop de sauvegardes en même temps.

Sélection de certains fichiers (correspondant à une recherche) à sauvegarder

En utilisant des caractères génériques,vous pouvez sauvegarder les fichiers correspondant à un critère spécifique.

> **REMARQUE :**
> Cette fonctionnalité n'est pas prise en charge par l'intégration de Data Protector avec le serveur NDMP.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**, puis le type de spécification approprié (par exemple **système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Sélectionnez la spécification de sauvegarde contenant l'objet cible.
4. Cliquez sur l'onglet **Résumé d'objet sauvegarde**.
5. Dans la page Résumé d'objet Sauvegarde, cliquez avec le bouton droit sur un objet sauvegarde, puis cliquez sur **Propriétés**.
6. Cliquez sur l'onglet **Arborescences/Filtres**, puis cliquez sur le bouton **Filtre**.
7. Dans la zone de texte Seulement, saisissez le critère à utiliser pour sauvegarder uniquement certains fichiers, puis cliquez sur le bouton **Ajouter**.

   Répétez cette étape si vous souhaitez utiliser d'autres critères.
8. Cliquez sur **OK**.

Fichiers ignorés lors de la sauvegarde

En utilisant des caractères génériques, vous pouvez ignorer les fichiers correspondant à un critère spécifique lors de la sauvegarde.

> **REMARQUE :**
> Cette fonctionnalité n'est pas prise en charge par l'intégration de Data Protector avec le serveur NDMP.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**, puis le type de spécification approprié (par exemple **système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Sélectionnez la spécification de sauvegarde contenant l'objet cible.
4. Cliquez sur l'onglet Résumé d'objet sauvegarde.
5. Dans la page Résumé de la Sauvegarde, cliquez avec le bouton droit sur un objet sauvegarde, puis cliquez sur Propriétés.
6. Cliquez sur l'onglet Arborescences/Filtres, puis cliquez sur le bouton Filtre
7. Dans la zone de texte Ignorer, saisissez le critère à utiliser pour ignorer certains fichiers (par exemple *.tmp) puis cliquez sur le bouton Ajouter.

   Répétez cette étape si vous souhaitez utiliser d'autres critères.
8. Cliquez sur **OK**.

Sélection de l'emplacement du raccourci pour le démarrage d'une sauvegarde

Vous pouvez créer un raccourci de la spécification de sauvegarde sélectionnée sur le disque que vous pouvez ensuite utiliser pour exécuter la sauvegarde sans utiliser l'interface utilisateur graphique Data Protector. Un double-clic sur ce raccourci permet d'ouvrir l'invite de commande et d'exécuter la commande `omnib` pour la spécification de sauvegarde sélectionnée.

Limites

- Le raccourci de démarrage d'une sauvegarde est pris en charge uniquement sur les systèmes Windows.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis le type de spécification de sauvegarde approprié (par exemple, **Système de fichiers**).
3. Cliquez sur la spécification de sauvegarde sélectionnée avec le bouton droit puis cliquez sur **Sélectionner l'emplacement pour le raccourci**. La boîte de dialogue Enregistrer sous s'affiche.
4. Entrez le nom et sélectionnez l'emplacement du raccourci, puis cliquez sur Enregistrer.

Le raccourci de démarrage d'une sauvegarde sélectionnée apparaît à l'emplacement sélectionné sur le disque.

Sauvegarde à l'aide de plusieurs Agents de disque

Lorsque vous sauvegardez des objets volumineux, vous pouvez accélérer le processus de sauvegarde en utilisant plusieurs Agents de disque.

Les points suivants peuvent contenir des informations supplémentaires :

- Dans la spécification de sauvegarde, vous devez définir manuellement les répertoires/fichiers à sauvegarder à l'aide d'un nouvel Agent de disque. Veillez à ne pas spécifier plusieurs fois les mêmes données.
- Lorsque plusieurs Agents de disque accèdent simultanément au même disque, la récupération des données depuis ce disque est moins performante. Cela peut être différent avec des baies de disques.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**.
3. Cliquez avec le bouton droit de la souris sur l'élément à sauvegarder (par exemple, **Système de fichiers**), puis sélectionnez **Ajouter sauvegarde**.

4. Dans la boîte de dialogue Créer sauvegarde, sélectionnez l'un des modèles disponibles, puis cliquez sur **OK** pour lancer l'assistant.
5. Dans la page de propriétés Source, ne sélectionnez pas des répertoires/fichiers situés sur le même disque logique ou point de montage si vous voulez les sauvegarder à l'aide de plusieurs Agents de disque. Toutefois, vous pouvez sélectionner des répertoires/fichiers à sauvegarder à l'aide d'un seul Agent de disque. Cliquez sur **Suivant**.
6. Dans la page de propriétés Destination, sélectionnez le(s) périphérique(s) à utiliser pour la sauvegarde. Cliquez sur **Suivant**.

   Vous pouvez également indiquer si vous souhaitez créer des copies supplémentaires (miroirs) de votre sauvegarde au cours de la session de sauvegarde. Indiquez le nombre de miroirs à créer et les périphériques à utiliser en cliquant sur **Ajouter un miroir** et **Supprimer un miroir**. Les périphériques utilisés pour la création de miroirs d'objet ne doivent pas être les mêmes que ceux employés pour la sauvegarde. La mise en miroir d'objets n'est pas prise en charge pour les sauvegardes ZDB sur disque et NDMP.
7. Dans la page de propriétés Options, paramétrez éventuellement d'autres options et cliquez sur **Suivant**.
8. Dans la page Résumé de sauvegarde, cliquez sur **Ajout manuel**.
9. Dans la boîte de dialogue Sélectionner objet sauvegarde, sélectionnez le type d'objet à sauvegarder (par exemple, **système de fichiers Windows**). Cliquez sur **Suivant**.
10. Dans la boîte de dialogue Sélection générale, sélectionnez le système client et le point de montage à sauvegarder. Il est également nécessaire de saisir une description. Cliquez sur **Suivant**.
11. Dans la boîte de dialogue Sélection Arborescences/Filtres, indiquez les répertoires et fichiers à sauvegarder ou à exclure de la sauvegarde. Les éléments que vous sélectionnez ici seront sauvegardés à l'aide d'un seul Agent de disque. Cliquez sur **Suivant**.
12. Dans les boîtes de dialogue Options générales, Options avancées et Options spécifiques d'objet Windows, paramétrez éventuellement d'autres options et cliquez sur **Suivant**, puis sur **Terminer**.
13. Répétez les étapes 9 à 13 pour les répertoires/fichiers à sauvegarder sur le point de montage à l'aide d'un autre Agent de disque.
14. Dans la page Résumé de sauvegarde, consultez le résumé de la spécification de sauvegarde, puis cliquez sur **Suivant**.
15. À la fin de l'assistant de sauvegarde, vous pouvez enregistrer, enregistrer et planifier, démarrer ou tester la sauvegarde configurée.

Traitement de petites sauvegardes récurrentes

Lorsque vous devez effectuer des sauvegardes récurrentes de nombreux petits objets, vous devez effectuer de nombreuses sessions de sauvegarde. Au cours de chacune de ces sessions, les supports sont chargés et déchargés du lecteur. Une sauvegarde de ce type est non seulement assez longue, mais elle entraîne aussi la détérioration des supports. Pour économiser les supports et gagner du temps, il est recommandé de créer un périphérique de bibliothèque de fichiers afin d'effectuer les petites sauvegardes récurrentes sur disque et non plus sur bande. Vous pouvez ensuite utiliser la fonctionnalité de copie d'objets pour déplacer les données du disque vers une bande.

Cette méthode permet de réaliser les sauvegardes plus rapidement et d'économiser les supports, car ceux-ci ne sont chargés et déchargés qu'une seule fois (au cours de la session de copie d'objets).

Pour réaliser des sauvegardes fréquentes d'un grand nombre d'objets de petite taille, effectuez les opérations suivantes :

1. Configurez un périphérique de bibliothèque de fichiers. Choisissez pour chaque module d'écriture la même taille de bloc que celle du périphérique qui sera utilisé lors de la deuxième étape.
2. Créez une spécification de sauvegarde pour tous les petits objets. Utilisez le périphérique de fichier créé au cours de la première étape pour la sauvegarde.
3. Exécutez la sauvegarde ou planifiez-la.
4. Utilisez la fonctionnalité de copie d'objets pour déplacer les données sauvegardées sur une bande.

Sauvegarde d'image de disque

Vous pouvez effectuer une sauvegarde d'image disque sur les plates-formes UNIX et Windows.

Une sauvegarde d'image disque est une sauvegarde ultra-rapide au cours de laquelle Data Protector sauvegarde les disques, partitions de disque ou volumes logiques sans suivre la structure des fichiers et répertoires stockés sur ces sources de données. Data Protector stocke la structure de l'image disque à un niveau de caractère.

Vous pouvez effectuer une sauvegarde d'image disque de certaines sections du disque ou de sa totalité.

> **REMARQUE :**
> Sur les systèmes Windows, la sauvegarde d'image disque est effectuée en utilisant des modules d'écriture VSS. Ainsi, le volume n'est pas verrouillé pendant la sauvegarde et d'autres applications peuvent y accéder. C'est particulièrement important lorsque vous sauvegardez un volume Système. La sauvegarde VSS d'image disque est activée par défaut. Pour personnaliser la sauvegarde VSS d'image disque, utilisez les options omnirc suivantes : `OB2_VSS_RAW_BACKUP`, `OB2_VSS_RAW_BACKUP_ALLOW_FALLBACK` et `OB2_VSS_SNAPSHOT_TIMEOUT`.

Quand faut-il utiliser une sauvegarde d'image disque ?

- Quand vous avez beaucoup de petits fichiers et qu'une sauvegarde rapide est nécessaire.
- Quand une sauvegarde de disque complète est nécessaire, par exemple, pour la récupération après sinistre ou avant une mise à jour logicielle majeure. Sur les systèmes Windows, la sauvegarde d'image disque peut être utilisée lors de la préparation EADR/OBDR.
- Lorsqu'une connexion directe de disque à disque n'est pas possible et que vous voulez dupliquer un système de fichiers sur un autre disque. Ce dernier doit être identique au disque d'origine.

Comment spécifier une section d'image disque ?

Sur les systèmes UNIX

- Pour indiquer une section d'image disque, utilisez le format suivant : `/dev/rdsk/Filename`, par exemple : `/dev/rdsk/c2t0do`
- Pour indiquer une section de volume logique brut, utilisez le format suivant : `/dev/vgNumber/rlvolNumber`, par exemple : `/dev/vg01/rlvol1`

Sur les systèmes Windows

Vous pouvez spécifier une section d'image disque de deux manières : la première sélectionne un volume donné et la seconde un disque entier. Dans le cas d'une sauvegarde avec temps d'indisponibilité nul, utilisez la seconde méthode :

- `\\.\DriveLetter`, par exemple : `\\.\E:`

  > **REMARQUE :**
  > Lorsque le nom du volume est indiqué comme lettre de lecteur, le volume n'est pas verrouillé pendant la sauvegarde. Un volume qui n'est pas monté ou monté comme un dossier NTFS ne peut pas être utilisé pour les sauvegardes d'images disque.

- `\\.\PHYSICALDRIVE#`, où # est le numéro du disque à sauvegarder. Par exemple : `\\.\PHYSICALDRIVE3`

Où trouver une section d'image disque ?

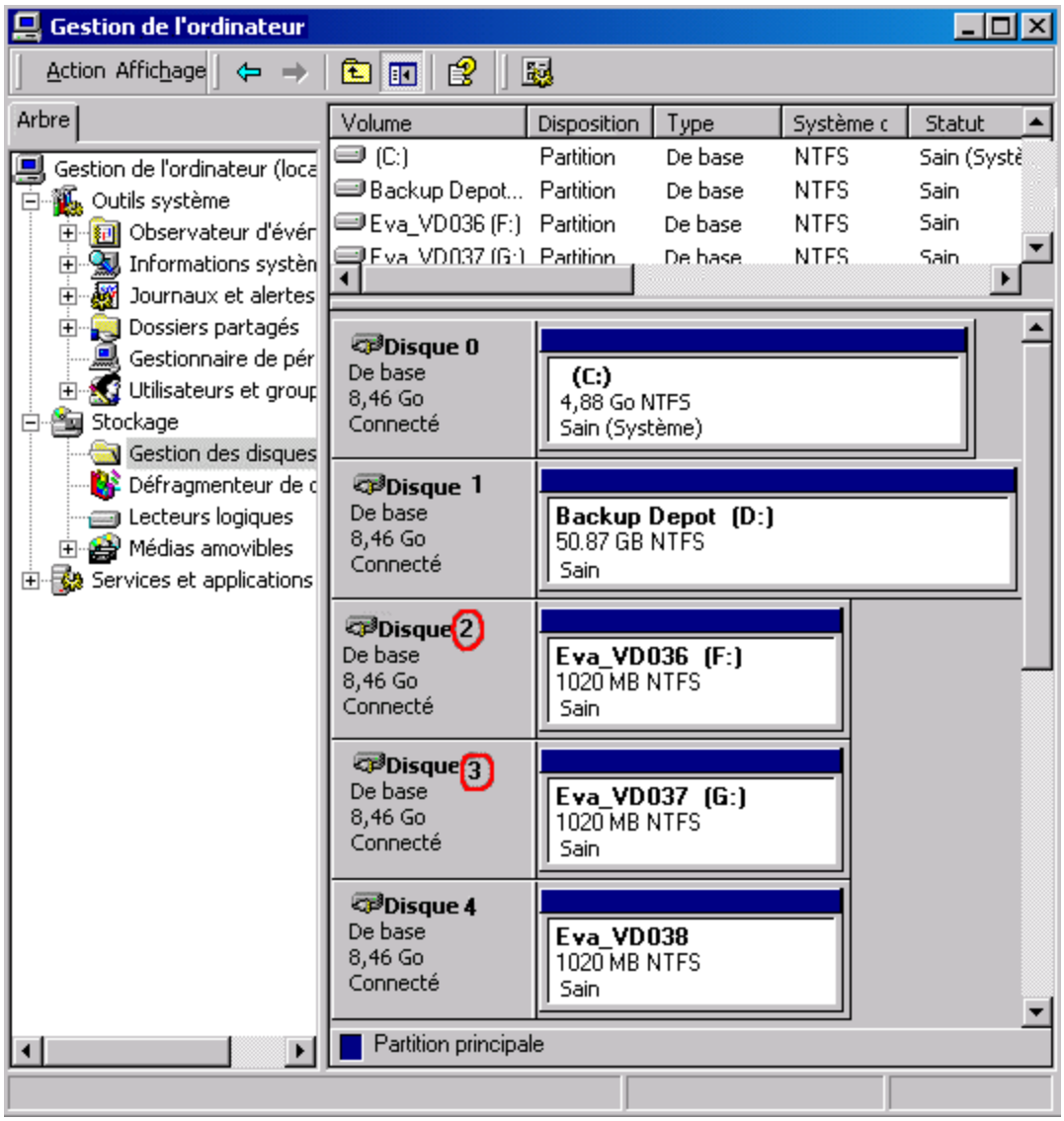
Sur les systèmes UNIX

Les sections d'image disque figurent généralement dans le répertoire `/dev/rdsk`. Les volumes logiques bruts se trouvent sous `/dev/vgNumber`. Dans les systèmes HP-UX, les volumes logiques bruts se trouvent sous `/dev/vgNumber`. La première lettre d'un volume logique brut est `r`, par exemple `/dev/vg01/rlvol2`.

Sur les systèmes Windows

Vous pouvez afficher le nombre actuel de vos disques (ainsi que les lettres de lecteurs) en cliquant sur **Outils d'administration** dans le Panneau de configuration, puis sur **Gestion de l'ordinateur**, **Stockage**, **Gestion des disques**.

Chiffres représentant des disques (nombre de lecteurs physiques) sur le système Windows



REMARQUE :
Sur les systèmes Windows, les chiffres représentant des disques peuvent varier si le système est redémarré.

Sauvegarde d'un client avec découverte des disques

Pour la sauvegarde d'un client avec découverte des disques, vous spécifiez un client en tant que source de données. Si un autre disque est ensuite monté, la sauvegarde va l'inclure. Alors qu'une sauvegarde de système de fichiers oblige à indiquer tout nouveau disque ajouté ou système de fichiers monté qui ne figure pas encore dans la spécification de sauvegarde, ceci n'est pas nécessaire en cas de découverte des disques.

Data Protector contacte le client lors de la sauvegarde et recherche tous les systèmes de fichiers sur les disques connectés au client. Chaque système de fichiers détecté (CONFIGURATION également sur les systèmes Windows) est ensuite sauvegardé de manière normale. La description de chaque

objet de système de fichiers est générée et le point de montage du système de fichiers est ajouté à la description de la sauvegarde du client.

Lors d'une sauvegarde avec découverte des disques, Data Protector ne sauvegarde que les disques réels. Par conséquent, sur les systèmes UNIX, Data Protector ne localise pas les NFS, les systèmes de fichiers montés sur CD et les points de montage amovibles. De même, sur les systèmes Windows, Data Protector ne localise pas les CD et les lecteurs contenant des supports amovibles.

Cas d'emploi de la découverte des disques

Ce type de sauvegarde concerne, en particulier, les environnements dynamiques où les configurations changent rapidement. Il est recommandé de l'utiliser dans les cas suivants :

- Si vous sauvegardez des stations de travail avec des disques de taille relativement réduite qui sont souvent montés ou démontés.
- Si vous souhaitez sauvegarder les données après un point de montage dans un répertoire, quel que soit le nombre des systèmes de fichiers montés. Par exemple, `/home/data`, où `/home/data/disk1` et `/home/data/newdisk/disk2` peuvent être montés ou démontés fréquemment et indépendamment l'un de l'autre.
- Si vous sauvegardez l'ensemble d'un système pour la préparation à une récupération après sinistre.

Spécification de sauvegarde

Si vous créez une spécification de sauvegarde qui utilisera une découverte des disques, cliquez sur la case à cocher en regard du nom du système client et pas sur celle en regard de ses disques (volumes). Une fois que vous avez sélectionné le système client, vous pouvez vérifier le type de sauvegarde configuré dans la page de propriétés Résumé d'objet sauvegarde. Sous l'étiquette `Type`, vous devriez voir `Client System`.

Sauvegarde d'un serveur Web

Pour sauvegarder un serveur Web, suivez la procédure de sauvegarde standard de fichiers, de répertoires et de clients. Vous devez également tenir compte des points suivants :

- Lors de la sauvegarde d'un client, Data Protector sauvegarde tout le serveur Web, mais pas les données stockées sur d'autres clients/serveurs. Afin que ces données soient sauvegardées, vous devez également les sélectionner pour la sauvegarde.
- Lors de la sauvegarde d'un système de fichiers, vous devez savoir où se trouvent tous les fichiers et répertoires du serveur Web ainsi que ses clients respectifs. Vous devez toujours inclure les fichiers de configuration Web ainsi que les répertoires racine correspondants.
- Data Protector sauvegarde tous les fichiers dont l'état est statique. Si des fichiers sont modifiés au cours de la sauvegarde, les modifications ne sont pas sauvegardées.

Si une base de données telle qu'Oracle ou Informix Server est présente sur le serveur Web, suivez la procédure de sauvegarde spécifique à la base de données.

Activation de la prise en charge Wake ONLAN

Si vos systèmes Windows prennent en charge Wake ONLAN , vous pouvez utiliser la prise en charge Wake ONLAN Data Protector.

Lorsqu'un Gestionnaire de session de sauvegarde ne parvient pas à se connecter à un client configuré pour utiliser la prise en charge Wake ONLAN, il envoie une demande de réveil conforme au protocole Wake ONLAN et effectue une nouvelle tentative de connexion. Ceci permet d'exploiter au mieux les fonctions d'économie d'énergie des ordinateurs, qui risqueraient sinon d'interférer avec le processus de sauvegarde.

Vous pouvez activer la prise en charge Wake ONLAN pour des ordinateurs dotés d'une interface réseau compatible Wake ONLAN, tels que ceux de la gamme HPE NightDIRECTOR. L'option Wake ONLAN (WOL) est disponible dans la configuration BIOS.

Quand vous installez un Agent de disque sur un client Windows et l'ajoutez à une cellule, l'adresse MAC du client est automatiquement détectée. Vous pouvez également modifier manuellement cette adresse.

Procédure

1. Dans la liste de contexte, cliquez sur **Clients**.
2. Dans la fenêtre de navigation, recherchez le client souhaité, cliquez dessus avec le bouton droit, puis cliquez sur Propriétés.
3. Cliquez sur l'onglet Avancé.
4. Sélectionnez l'option Activer Wake ONLAN. Si nécessaire, modifiez l'adresse MAC.
5. Cliquez sur **Appliquer**.

À propos des modèles de sauvegarde

Des modèles de sauvegarde Data Protector peuvent vous aider à simplifier la manipulation de (nombreuses) spécifications de sauvegarde et d'options associées. Un modèle est un jeu d'options clairement définies pour une spécification de sauvegarde, qui peut servir de base à la création et la modification des spécifications.

Le but d'un modèle est de configurer plusieurs spécifications de sauvegarde avec différents objets, utilisées de la même façon (un paramètre d'option commun pour des éléments particuliers comme les options de périphérique et/ou de système de fichiers).

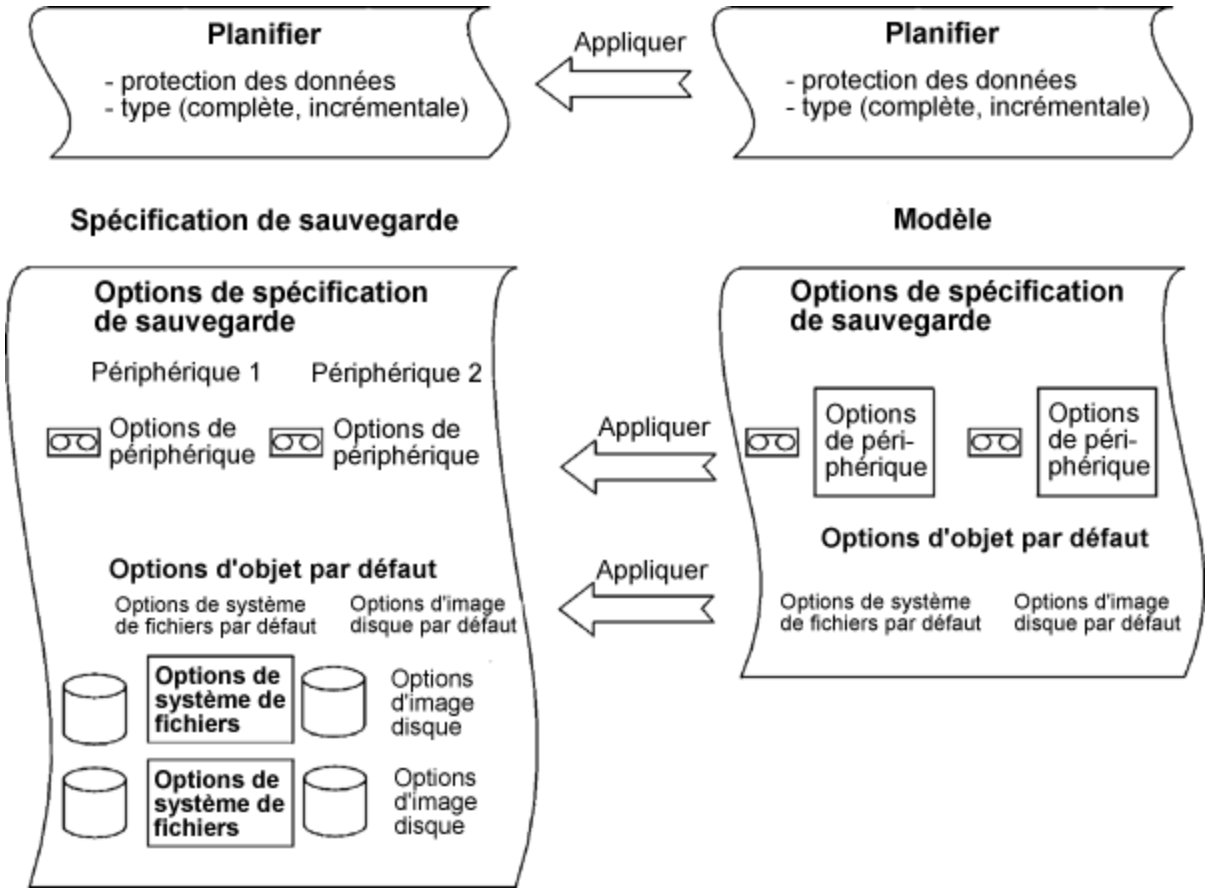
Data Protector vous propose des modèles par défaut pour différents types de données (système de fichiers, Exchange etc.) sans spécifier des objets, des périphériques, des options ni une planification. Les modèles de sauvegarde vides (système de fichiers, Informix, etc.) ne contiennent aucun objet ou périphérique sélectionné. Les options de spécification de sauvegarde et les options d'objet ont des valeurs par défaut Data Protector et aucune planification n'est définie.

Les modèles sont créés et modifiés de façon similaire aux sauvegardes, à la seule différence que les éléments, tels que les objets, ne sont pas sélectionnés dans le modèle de sauvegarde. Il est possible d'appliquer un modèle à des spécifications de sauvegarde existantes ou de l'utiliser lors de la création

d'une sauvegarde. Si vous modifiez ensuite le modèle, vous devez l'appliquer de nouveau pour que les modifications prennent effet.

> **CONSEIL :**
> Positionnez votre curseur sur un modèle pour afficher une fenêtre contextuelle contenant la description de celui-ci.

Application des options de sauvegarde



Création d'un modèle de sauvegarde

Vous pouvez créer un modèle de sauvegarde avec des paramètres spéciaux afin de l'adapter à un environnement spécifique.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément Modèles.
3. Cliquez avec le bouton droit sur le type de modèle à créer (par exemple Système de fichiers), puis cliquez sur Ajouter modèle pour ouvrir l'assistant.

4. Suivez les indications de l'assistant. Celui-ci vous permet de sélectionner le périphérique de sauvegarde à utiliser, de définir les options et de planifier les sauvegardes.

Le nouveau modèle est disponible lors de la création d'une nouvelle spécification de sauvegarde ou lors de l'application d'un modèle à une ou plusieurs spécifications de sauvegarde.

Modification d'un modèle de sauvegarde

Il est possible de modifier un modèle de sauvegarde. Si vous voulez que votre spécification de sauvegarde soit modifiée en fonction du modèle, vous devez appliquer celui-ci à nouveau car les spécifications de sauvegarde ne sont pas automatiquement mises à jour.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Modèles**, puis le type de modèle que vous souhaitez modifier (par exemple **Système de fichiers**). Tous les modèles enregistrés du type sélectionné s'affichent alors.
3. Cliquez avec le bouton droit sur le modèle à modifier, puis cliquez sur **Propriétés**.
4. Dans les pages de propriétés du modèle, modifiez-le, puis cliquez sur Appliquer.

Une fois que vous avez modifié votre modèle de sauvegarde, vous pouvez l'appliquer à une spécification de sauvegarde ou l'utiliser pour en créer une nouvelle.

Copie d'un modèle de sauvegarde

Vous pouvez copier un modèle de sauvegarde.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Modèles** puis développez le type de modèle de sauvegarde approprié (par exemple **Système de fichiers**). Tous les modèles de sauvegarde enregistrés s'affichent alors.
3. Dans la zone de résultats, cliquez avec le bouton droit sur le modèle à copier, puis cliquez sur **Copier sous**. La boîte de dialogue Copier sauvegarde sous s'affiche.
4. Dans la zone de texte Nom, attribuez un nom au modèle copié. Dans la liste déroulante Groupe, sélectionnez éventuellement un autre groupe pour le modèle copié.
5. Cliquez sur **OK**.

Le modèle de sauvegarde copié est affiché dans la fenêtre de navigation et dans la zone de résultats.

Suppression d'un modèle de sauvegarde

Vous pouvez supprimer un modèle de sauvegarde.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Modèles** puis développez le type de modèle de sauvegarde approprié (par exemple **Système de fichiers**). Tous les modèles de sauvegarde enregistrés s'affichent alors.
3. Cliquez avec le bouton droit sur le modèle à supprimer, puis cliquez sur **Supprimer**. Confirmez ensuite votre choix.

Le modèle de sauvegarde est supprimé.

Application d'un modèle de sauvegarde à une spécification de sauvegarde

Vous pouvez appliquer un modèle à une ou à plusieurs spécifications de sauvegarde. Dans ce cas, vous pouvez sélectionner les groupes d'options à appliquer.

> **REMARQUE :**
> Si vous appliquez un modèle de sauvegarde à une spécification de sauvegarde existante et sélectionnez les options Système de fichiers et/ou Planifier, les paramètres de protection du modèle remplacent ceux de la spécification.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**.
3. Cliquez avec le bouton droit de la souris sur une spécification de sauvegarde enregistrée, puis sélectionnez **Appliquer modèle**.
4. Dans la boîte de dialogue **Appliquer modèle**, sélectionnez le modèle que vous souhaitez appliquer à la spécification de sauvegarde.

   > **CONSEIL :**
   > Vous pouvez désélectionner certaines options du modèle (**Arborescences**, **Options de sauvegarde**, **Périphérique**, etc.), afin qu'elles ne soient pas appliquées à la spécification de sauvegarde sélectionnée.

   > **REMARQUE :**
   > Pour appliquer un modèle à une spécification de sauvegarde d'intégration, il est nécessaire que la spécification de sauvegarde ne soit pas ouverte dans la zone de résultats. Si vous cliquez d'abord sur la spécification de sauvegarde pour l'ouvrir, puis tentez d'appliquer le modèle à cette spécification de sauvegarde, l'option **Appliquer modèle** n'est pas disponible.

5. Cliquez sur **OK** pour appliquer le modèle à la spécification de sauvegarde.

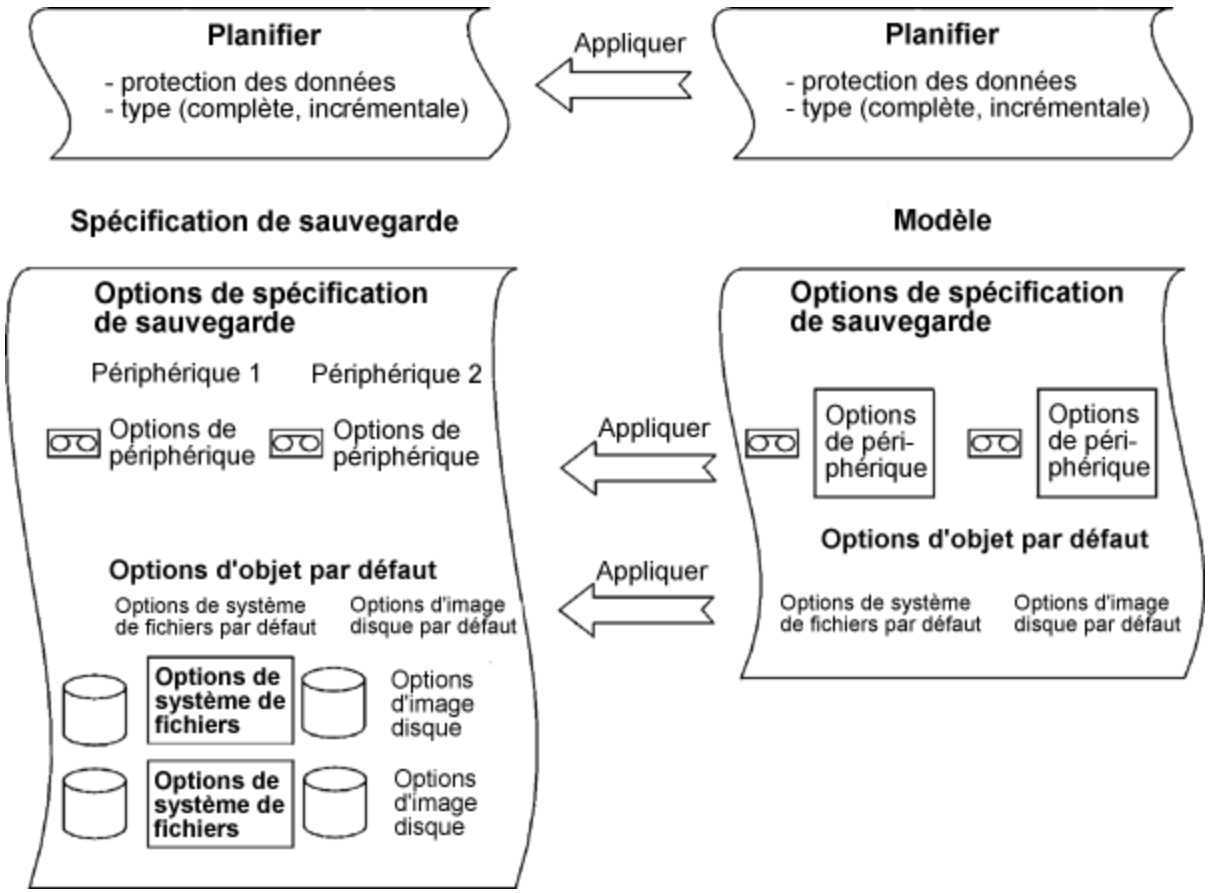
Une fois les options du modèle appliquées, vous pouvez modifier la spécification de sauvegarde et les paramètres.

À propos des options de sauvegarde

Data Protector propose un ensemble complet d'options de sauvegarde qui permettent de définir une sauvegarde de façon très précise. Toutes ces options possèdent des valeurs par défaut (sélectionnées ou désélectionnées) adaptées à la plupart des situations.

La disponibilité des options de sauvegarde dépend du type de données sauvegardées. Par exemple, vous ne disposerez pas des mêmes options pour la sauvegarde d'un système de fichiers que pour celle d'une image disque. Les options courantes et spécifiques qui se trouvent dans les pages de propriétés pour Exchange, SQL, etc., sont décrites dans l'aide contextuelle pour chaque type de sauvegarde spécifique.

Application des options de sauvegarde



Options de sauvegarde disponibles

Le jeu d'options suivant est disponible lorsque vous sauvegardez des données :

Options de spécification de sauvegarde

Ces options s'appliquent à l'ensemble de la spécification de sauvegarde, quel que soit le type d'objet sauvegarde.

Options du système de fichiers

Ces options s'appliquent à chaque objet de la sauvegarde d'un système de fichiers. Vous pouvez également modifier les options d'objets spécifiques. Les paramètres d'objets spécifiques remplacent les paramètres par défaut.

Options d'image disque

Ces options s'appliquent à chaque objet d'une sauvegarde d'image disque (rawdisk). Vous pouvez également modifier les options d'un objet spécifique. Les paramètres d'objets spécifiques remplacent les paramètres par défaut.

Options de périphérique

Ces options définissent le comportement des périphériques de sauvegarde. Si vous ne les définissez pas, les valeurs sont lues en prenant en compte la définition du périphérique.

Options de planification

Pour chaque sauvegarde planifiée particulière ou périodique, vous pouvez indiquer son type (complète ou incrémentale ; d'autres types de sauvegarde sont disponibles pour certaines intégrations), la charge réseau et la protection de données. Avec ZDB, vous pouvez sélectionner ZDB sur disque + bande ou ZDB sur disque (si restauration instantanée est activée).

La protection de données qui est spécifiée dans l'assistant Planifier remplace tout autre paramètre de protection dans la spécification de sauvegarde.

Options les plus fréquemment utilisées

Voici la liste des options généralement modifiées conformément aux stratégies de sauvegarde spécifiques.

- Protection des données
- Protection de catalogue
- Journalisation
- Partage de charge
- Propriété

Protection des données : Combien de temps les données sont-elles conservées sur le support

Il est extrêmement important de configurer des stratégies de protection pour garantir la sécurité des données et la bonne gestion de votre environnement. Vous devez spécifier la durée pendant laquelle vos données sauvegardées sont conservées sur le support en fonction de vos stratégies d'entreprise

en matière de protection des données. Par exemple, vous pouvez décider que les données deviennent obsolètes après trois semaines et peuvent être écrasées par une sauvegarde ultérieure.

Vous pouvez appliquer une protection des données à différents endroits. Différentes combinaisons sont disponibles, selon que vous exécutez une sauvegarde interactive, démarrez une spécification de sauvegarde enregistrée ou planifiez une sauvegarde. La valeur par défaut est Permanent.

Sauvegardes interactives

Lors de la configuration d'une sauvegarde interactive, vous pouvez modifier la protection des données par défaut pour l'ensemble de la sauvegarde. En outre, vous pouvez spécifier différentes périodes de protection des données pour des objets de sauvegarde individuels. La protection spécifiée au niveau de l'objet de sauvegarde remplace le paramètre de protection par défaut.

Sauvegardes avec une spécification de sauvegarde enregistrée

Lors du lancement de sauvegardes enregistrées à l'aide de l'interface graphique, la protection des données est appliquée comme indiqué pour les sauvegardes interactives.

Lors du lancement de sauvegardes enregistrées à l'aide de l'interface de ligne de commande, vous pouvez également spécifier la protection des données. Cette définition remplace tous les paramètres de protection de données dans la spécification de sauvegarde.

Sauvegardes planifiées

Vous pouvez indiquer une période de protection différente pour chaque sauvegarde planifiée périodique ou individuelle. La protection de données indiquée dans l'assistant Planifier remplace tous les autres paramètres de protection de données dans la spécification de sauvegarde. Si vous conservez la protection par défaut, la protection des données est appliquée comme indiqué pour les sauvegardes interactives.

Catalog protection : Combient de temps les données sont-elles conservées dans l'IDB

Vous pouvez définir indépendamment la protection de catalogue et la protection des données. Lorsque la protection des données se termine et qu'un support est écrasé, les catalogues des objets sont supprimés, quelle que soit la protection de catalogue définie.

La protection de catalogue, combinée au niveau de journalisation, affecte considérablement la croissance de l'IDB, l'exploration des données à restaurer et les performances de la sauvegarde. Il est important de définir une stratégie de protection de catalogue adaptée à votre environnement. La protection de catalogue n'a aucun effet si le niveau de journalisation est défini sur Pas de journalisation.

Si la protection de catalogue est permanente, les informations figurant dans l'IDB sont supprimées uniquement lorsque des supports sont exportés ou effacés. Dans ce cas, la taille de l'IDB croît de manière linéaire jusqu'à ce que la période de protection des données soit atteinte, même si le nombre de fichiers dans la cellule ne change pas.

La valeur par défaut est **Comme la protection de données**. Cela signifie que vous pouvez rechercher et sélectionner des fichiers ou des répertoires aussi longtemps que les supports sont disponibles pour la restauration.

En raison des limites des systèmes d'exploitation, la date de la dernière protection qui peut être définie est fixée au 18 janvier 2038.

Protection du catalogue expirée

Lorsque la protection du catalogue arrive à expiration, les informations ne sont pas immédiatement supprimées de l'IDB. Data Protector les supprime automatiquement une fois par jour. Les informations de l'IDB étant organisées par support, elles ne sont supprimées que lorsque la protection de catalogue expire pour tous les objets du support.

Lorsque la protection du catalogue arrive à expiration, la restauration des données reste possible, mais vous devez spécifier manuellement les noms de fichiers.

Protection de catalogue et sauvegarde

Les paramètres de protection de catalogue n'ont aucun impact sur les performances de la sauvegarde.

Protection de catalogue et restauration

Lorsque la protection de catalogue expire, les données sont restaurées comme si elles étaient sauvegardées en utilisant l'option No Log.

Logging : Modifications des détails concernant les données stockées dans l'IDB

Le niveau de journalisation Data Protector détermine la quantité de détails sur les fichiers et répertoires écrits dans l'IDB pendant la sauvegarde. Quatre niveaux de journalisation sont disponibles :

- Journaliser tout
- Fichiers journal
- Répertoires journal
- Pas de journalisation

HPE recommande d'utiliser différents niveaux de journalisation dans la même cellule. Une cellule se compose souvent d'un serveur de messagerie (ou équivalent) qui génère quotidiennement un grand nombre de fichiers, de serveurs de base de données qui stockent toutes les informations dans une poignée de fichiers, et de quelques postes de travail utilisateur. Les variations de ces systèmes étant assez différentes, il est difficile de recommander une configuration adaptée à tous ces cas. HPE recommande de créer plusieurs spécifications de sauvegarde avec les réglages de niveau de journalisation suivants :

- Pour les serveurs de messagerie, utilisez l'option Journaliser répertoires.
- Pour les serveurs de bases de données, utilisez l'option Pas de journalisation car l'exploration de fichiers individuels n'a aucun sens dans ce cas.
- Pour les stations de travail, utilisez l'option Journaliser fichiers afin de pouvoir rechercher et restaurer différentes versions des fichiers.
- L'option Journaliser tout permet d'afficher les attributs de fichiers tels que la date de modification et les ACL.

Niveau de journalisation et vitesse de sauvegarde

La vitesse de sauvegarde est approximativement la même quel que soit le niveau de journalisation choisi.

Niveau de journalisation et exploration des données à restaurer

La modification du niveau d'informations stockées affecte votre capacité à parcourir les fichiers dans l'interface graphique de Data Protector pendant une restauration. Si l'option **Pas de journalisation** est sélectionnée, l'exploration n'est pas possible ; si l'option **Journaliser répertoires** est sélectionnée, l'exploration des répertoires est possible ; si l'option **Journaliser fichiers** est sélectionnée, une exploration complète est possible mais les attributs de fichiers (taille, date de création et de modification, etc.) ne sont pas affichés.

Si vous connaissez les noms des fichiers que vous souhaitez restaurer, vous pouvez toujours les spécifier manuellement au lieu de les rechercher, quel que soit le niveau de journalisation appliqué.

Niveau de journalisation et vitesse de restauration

La vitesse de restauration est approximativement la même lorsque la session de sauvegarde correspondante a été lancée avec soit le niveau de journalisation **Log All**, **Log Directories**, ou **Log Files**.

Si la session de sauvegarde a été exécutée avec le niveau de journalisation **Pas de journalisation**, la vitesse peut diminuer lors de la restauration de fichiers individuels. Dans ce cas, Data Protector doit lire toutes les données à partir du début de l'objet avant de trouver un fichier à restaurer.

Dans le cas d'une restauration de système complet, tout l'objet de sauvegarde est lu de toute façon, ainsi le niveau de journalisation ne joue pas un rôle important.

Equilibre de charge : Equilibre de l'utilisation des dispositifs de sauvegarde

Utilisez l'option Partage de charge si vous souhaitez sauvegarder un grand nombre d'objets sur un certain nombre de périphériques disponibles et souhaitez que Data Protector maintienne en permanence tous les périphériques occupés. Vous devez utiliser le partage de charge afin de minimiser l'impact des périphériques non disponibles sur la sauvegarde.

Désactivez l'option Partage de charge si vous souhaitez sauvegarder un petit nombre d'objets, si les objets sont sauvegardés sur des périphériques simples (DDS, par exemple), si vous voulez sélectionner manuellement les périphériques sur lesquels les objets seront sauvegardés, ou si vous voulez savoir sur quels supports les objets seront sauvegardés.

Les objets sont affectés à un périphérique disponible dans la liste des périphériques répertoriés dans la spécification de sauvegarde du partage de charge. Le premier périphérique est démarré et le nombre d'objets sélectionnés est défini selon sa simultanéité. Le périphérique suivant est démarré et les objets sont sélectionnés jusqu'à ce qu'il n'y ait plus d'objets dans la liste ou jusqu'au démarrage du nombre maximum de périphériques.

Si un périphérique devient indisponible, seuls les objets sauvegardés sur celui-ci au moment de la défaillance sont annulés. Tous les objets sauvegardés sur le périphérique avant la défaillance sont effectivement sauvegardés. Si la spécification de sauvegarde contient d'autres périphériques et que le nombre maximum de périphériques n'a pas été atteint, un nouveau périphérique démarre. Un périphérique peut devenir indisponible dans les cas suivants :

- défaillance lors d'une sauvegarde
- arrêt lors d'une sauvegarde

- utilisation par une autre session
- démarrage impossible

Le nombre d'objets à sauvegarder est atteint selon les critères suivants :

- Les objets situés sur le client connecté au périphérique de sauvegarde ont une priorité plus élevée.
- Les objets sont sélectionnés de telle sorte que le nombre d'Agents de disque par client reste aussi faible que possible.
- La taille des objets ne joue aucun rôle dans l'affectation d'un objet à un périphérique.

Les règles suivantes doivent être prises en compte lors de l'application des options du périphérique à partir d'un modèle :

- Si l'option Partage de charge n'est pas sélectionnée dans le modèle, les périphériques ne sont pas utilisés avec la spécification de sauvegarde.
- Si l'option Partage de charge est sélectionnée dans le modèle et dans la spécification de sauvegarde, les options du périphérique sont appliquées.
- Si l'option Partage de charge est sélectionnée uniquement dans le modèle, les options du périphérique ne seront appliquées que si la spécification de sauvegarde ne contient aucun périphérique.

Possession : Qui peut restaurer

A qui appartient une session de sauvegarde ?

Chaque session de sauvegarde et toutes les données sauvegardées qu'elle contient est affectée à un propriétaire. Il peut s'agir de l'utilisateur qui lance une sauvegarde interactive, du compte sous lequel le processus CRS est exécuté ou de l'utilisateur désigné comme propriétaire dans les options de la spécification de sauvegarde.

Si un utilisateur démarre une spécification de sauvegarde existante sans la modifier, la session n'est pas considérée comme interactive.

Si une spécification de sauvegarde modifiée est démarrée par un utilisateur, celui-ci est le propriétaire, à moins que les conditions ci-après soient remplies :

- L'utilisateur possède le droit utilisateur Permuter propriété de session.
- Le propriétaire d'une session de sauvegarde est explicitement défini dans la spécification de sauvegarde, avec le nom d'utilisateur, le groupe, le nom de domaine et le nom du système.

Si une sauvegarde est prévue sur un Responsable de Cellule UNIX, le titulaire de la session est `root:sys`, sauf si les conditions ci-dessus sont vraies.

Si vous prévoyez d'effectuer une sauvegarde sur un Gestionnaire de cellule Windows, le propriétaire de la session est l'utilisateur spécifié lors de l'installation, à moins que les conditions indiquées ci-dessus soient remplies.

Pourquoi changer le propriétaire d'une sauvegarde ?

Vous pouvez changer le propriétaire d'une sauvegarde si l'administrateur configure et planifie une spécification de sauvegarde, et si les opérateurs sont autorisés à l'exécuter, mais qu'ils ne peuvent pas la modifier ou l'enregistrer. Si l'option de sauvegarde privée est définie pour tous les objets, les

opérateurs ne pourront rien restaurer, mais ils pourront toujours gérer les sauvegardes et redémarrer les sessions ayant échoué.

Si la configuration de sauvegarde est modifiée mais pas enregistrée, la sauvegarde est traitée comme une sauvegarde interactive et le propriétaire ne change pas. Si vous démarrez de façon interactive une sauvegarde incrémentale et que vous n'êtes pas le propriétaire de la sauvegarde complète, vous obtenez une autre sauvegarde complète au lieu de la sauvegarde incrémentale.

Qui peut restaurer un objet privé ?

Sauf si un objet est marqué comme étant Public, seuls les utilisateurs suivants peuvent restaurer l'objet :

- Les membres du groupe d'utilisateur `Admin` et `Operator`.
- Le propriétaire de la session de sauvegarde qui possède le droit Démarrer la restauration. D'autres droits utilisateur peuvent être nécessaires, notamment Restaurer vers un autre client.
- Les utilisateurs qui possèdent le droit Voir objets privés.

Le droit de voir et de restaurer des objets privés peut être attribué aux groupes autres que `admin` ou `operator`.

Options de spécification de sauvegarde

Ces options s'appliquent à l'ensemble de la spécification de sauvegarde, quel que soit le type des objets sauvegarde.

L'option de base est **Partage de charge** Par défaut, cette option est activée dans la boîte de dialogue Créer sauvegarde. Si vous la désactivez dans cette boîte de dialogue, vous pouvez la sélectionner ultérieurement dans la page de propriétés Destination de la spécification de sauvegarde, dans l'onglet Sauvegarde.

Pour plus d'informations sur les options de spécification de sauvegarde, reportez-vous au Aide de HPE Data Protector.

Options de spécification de sauvegarde générales

- Description
- Sur client
- Post-exécution
- Pré-exécution
- Reconnecter les connexions rompues
- Propriété

Options de spécification de sauvegarde pour la gestion des clusters

Redémarrage automatique de session

Si un basculement de l'application Data Protector compatible cluster survient pendant la sauvegarde, toutes les sessions de sauvegarde en cours et en attente échouent. Les options suivantes définissent le comportement de Data Protector après le basculement :

- Ne pas redémarrer les sauvegardes après basculement
- Redémarrer la sauvegarde de tous les objets
- Redémarrer la sauvegarde des objets ayant échoué

Paramètres d'abandon de session et d'ID d'abandon

Lorsqu'une application compatible cluster autre que Data Protector est exécutée sur un autre noeud que Data Protector et bascule sur le noeud sur lequel Data Protector est exécuté, il est possible de contrôler la charge sur ce système. Les options suivantes combinées avec la commande `omniclus` définissent le comportement de Data Protector après le basculement.

- Ne pas contrôler le temps de session écoulé
- Abandonner si inférieur à
- Abandonner si supérieur à
- Ne pas contrôler l'ID d'abandon
- Contrôler en fonction de l'ID d'abandon

Options de spécification de sauvegarde EMC Symmetrix

Systèmes client

- Système d'application
- Système de sauvegarde

Type de miroir

- TimeFinder
- Symmetrix Remote Data Facility
- Combinaison [SRDF + TimeFinder]

Pré-exécution et post-exécution de Split Mirror EMC Symmetrix

- Pré-exécution du Split Mirror
- Post-exécution du Split Mirror

Options EMC Symmetrix

- Découvrir environnement Symmetrix
- Rétablir les liens avant la sauvegarde
- Rétablir les liens après la sauvegarde

Options de spécification de sauvegarde Famille de baies de disque HPE P9000 XP

Systèmes client

Cet ensemble d'options ne peut être modifié qu'après enregistrement de la spécification de sauvegarde.

- Système d'application
- Système de sauvegarde

Type de miroir

- HPE Business Copy P9000 XP
- HPE Continuous Access P9000 XP
- Combinaisons (HPE Continuous Access P9000 XP + HPE Business Copy P9000 XP)
- Numéro(s) de MU

Options de gestion de réplique

- Conserver la réplique après la sauvegarde
- Suivre la réplique pour la restauration instantanée

Au début de la session

- Synchroniser les disques s'ils ne le sont pas déjà
- Abandonner la session si les disques miroir ne sont pas déjà synchronisés

À la fin de la session

- Préparer le prochain disque pour la sauvegarde (resynchroniser)

Options du système d'application

- Démonter les systèmes de fichiers du système d'application
- Arrêter/mettre en attente la ligne de commande de l'application
- Réactiver la ligne de commande de l'application

Options du système de sauvegarde

- Utiliser les mêmes points de montage que sur le système d'application
- Racine du chemin de montage sur le système de sauvegarde
- Ajouter des répertoires au chemin de montage
- Démonter automatiquement les systèmes de fichiers aux points de montage de destination
- Laisser le système de sauvegarde activé
- Activer le système de sauvegarde en mode lecture/écriture

Options de spécification de sauvegarde Famille de baies de disques HPE P6000 EVA

Systèmes client

- Système d'application
- Système de sauvegarde

Mode de réplication

- HPE Business Copy P6000 EVA
- HPE Continuous Access P6000 EVA + HPE Business Copy P6000 EVA

Traitement des répliques lors des scénarios de basculement

- Suivre le sens de réplication
- Gérer l'emplacement des répliques

Options de gestion des snapshots

- Source du snapshot
- Type de snapshot
- Niveau de redondance
- Reporter la sauvegarde sur bande de n minutes au maximum si les snapclones ne sont pas complètement créés

Préparation/synchronisation des mirrorclones

- Au début de la session
- A la fin de la session

Options de gestion de réplique

- Conserver la réplique après la sauvegarde
- Nombre de répliques en rotation
- Suivre la réplique pour la restauration instantanée

Options du système d'application

- Démonter les systèmes de fichiers du système d'application avant la génération de la réplique
- Arrêter/mettre en attente la ligne de commande de l'application
- Réactiver la ligne de commande de l'application

Options du système de sauvegarde

- Utiliser les mêmes points de montage que sur le système d'application
- Racine du chemin de montage sur le système de sauvegarde
- Ajouter des répertoires au chemin de montage
- Démonter automatiquement les systèmes de fichiers aux points de montage de destination
- Laisser le système de sauvegarde activé
- Activer le système de sauvegarde en mode lecture/écriture

Options du système de fichiers

Ces options s'appliquent à chaque objet de la sauvegarde d'un système de fichiers.

L'option de base est Protection.

Quatre ensembles d'options de système de fichiers **Avancé** apparaissent.

- Options du système de fichiers
- Autres options du système de fichiers
- WinFS, options du système de fichiers

Pour plus d'informations sur les options du système de fichiers, reportez-vous au Aide de HPE Data Protector.

Options du système de fichiers

- Protection de catalogue
- Post-exécution
- Pré-exécution
- Public
- Niveau de rapport

Autres options du système de fichiers

- Sauvegarder fichiers de taille
- Sauvegarder les liens réels POSIX en tant que fichiers
- Sauvegarder les liens réels POSIX en tant que fichiers
- Copier l'intégralité de l'image DR sur le disque
- **Sécurité des données**
  - Aucune
  - AES 256 bits
  - Encoder
- Afficher infos statistiques
- Ne pas conserver les attributs de temps d'accès
- Sauvegarde incrémentale avancée
- Utiliser le fournisseur de journaux des modifications du système de fichiers natif s'il est disponible
- Verrouiller les fichiers pendant la sauvegarde
- Journalisation

  Le niveau de journalisation Data Protector détermine la quantité de détails sur les fichiers et répertoires sauvegardés qui seront écrits dans la Base de données internes pendant la sauvegarde. Quatre niveaux de journalisation sont disponibles :
  - Journaliser tout
  - Fichiers journal
  - Répertoires journal
  - Pas de journalisation
- Compression logicielle

WinFS, options du système de fichiers

- Lecture asynchrone
- Sauvegarder les informations de partage pour les répertoires
- Détecter liens réels NTFS
- Ne pas utiliser l'attribut archive(D)
- **Fichiers ouverts**
  - Nombre de tentatives
  - Délai
- Déclarer fichiers verrouillés ouverts comme

- **Options de MS Volume Shadow Copy**
  - Utiliser Shadow Copy
  - Autoriser la reprise

Options d'image disque

Ces options s'appliquent à tous les objets image disque que vous sélectionnez pour la sauvegarde.

L'option de base est Protection.

Pour plus d'informations sur les options d'image disque, reportez-vous au Aide de HPE Data Protector.

Vous pouvez définir les options d'image disque Avancées :

- Protection de catalogue
- **Sécurité des données**
  - Aucune
  - AES 256 bits
  - Encoder
- Afficher infos statistiques
- Post-exécution
- Pré-exécution
- Public
- Niveau de rapport
- Compression logicielle

Options de périphérique

Vous pouvez définir ces options pour le périphérique de sauvegarde sélectionné dans une spécification de sauvegarde spécifique. Ces options constituent un sous-ensemble des options à définir lors de la configuration d'un périphérique de sauvegarde ou de la modification de ses propriétés. Les options dont la liste est donnée ci-dessous sont valides pour une spécification de sauvegarde particulière. Elles écrasent les options définies dans le contexte Périphériques Supports, qui s'appliquent globalement à ce périphérique particulier.

Pour plus d'informations sur les options de périphérique, reportez-vous au Aide de HPE Data Protector.

Propriétés du périphérique - Général

- Contrôle CRC
- Simultanéité
- Cryptage sur lecteur
- Pool de supports

- Liste de préallocation
- Nouvelle analyse

Options de planification

Lors de la planification d'une sauvegarde, vous pouvez définir des options supplémentaires. Pour chaque sauvegarde planifiée, vous pouvez spécifier le type de sauvegarde (complète ou incrémentale ; d'autres types de sauvegarde sont disponibles pour des intégrations spécifiques), la protection de données, la priorité, la charge de réseau, le schéma de récurrence et la durée estimée. Avec ZDB, vous pouvez sélectionner ZDB sur disque + bande ou ZDB sur disque (si restauration instantanée est activée).

La Protection de données spécifiée dans le planificateur prévaut sur les paramètres de protection définis ailleurs dans la spécification de sauvegarde.

Pour plus d'informations sur la création et la modification de planifications dans Data Protector à l'aide du planificateur, voir *Planificateur, Page 110*.

Options de session

- **Type de sauvegarde**
  - Complète
  - Incrémentale
- Protection de sauvegarde
- Priorité
- Charge réseau
- Schéma de récurrence
- Durée estimée

Sauvegarde Split Mirror/Snapshot

(disponible avec ZDB, mais uniquement en cas de sauvegarde ZDB sur disque + bande ou ZDB sur disque (restauration instantanée activée).

Définition des options de sauvegarde

Vous pouvez définir des options de sauvegarde lorsque vous créez une spécification de sauvegarde. Pour cela, vous devez accéder à la page de propriétés Options en suivant les indications de l'assistant.

Vous pouvez également définir des options de sauvegarde pour une spécification que vous avez déjà enregistrée.

> **REMARQUE :**
> Les options d'objet (système de fichiers et image disque) sont définissables à deux niveaux. Vous pouvez d'abord définir séparément les *options d'objet par défaut* pour tous les systèmes

de fichiers et toutes les images disque dans la spécification de sauvegarde. Vous pouvez ensuite les définir différemment pour un *objet particulier*. Ces valeurs remplacent alors celles par défaut. Par exemple, pour compresser les données de tous les clients à l'exception d'un client doté d'une UC lente, activez l'option **Compression** lorsque vous configurez les options de système de fichiers. Sélectionnez ensuite le client lent et désactivez la **compression** pour celui-ci.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécifications de sauvegarde**, puis le type de spécification de sauvegarde (par exemple **Système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez deux fois sur la spécification de sauvegarde dont vous souhaitez définir les options, puis cliquez sur l'onglet **Options**.
4. Dans la page Options, définissez les options comme vous le souhaitez. Cliquez sur l'un des boutons **Avancé** pour configurer les options avancées (selon le type d'options que vous souhaitez définir).

   Outre les options de spécification de sauvegarde, vous pouvez définir des options de système de fichiers, des options d'image disque, etc., selon le type de données pour lequel la spécification est configurée.
5. Recherchez l'option souhaitée, puis sélectionnez-la ou désélectionnez-la, ou saisissez les informations nécessaires.
6. Cliquez sur **OK** puis sur **Appliquer** pour enregistrer les modifications.

Indication d'une protection de données

Vous pouvez indiquer la protection des données lorsque vous exécutez des sauvegardes interactives, démarrez des spécifications de sauvegarde enregistrées ou planifiez des sauvegardes. La valeur par défaut est Permanent.

REMARQUE :
En raison des limites des systèmes d'exploitation, la date de la dernière protection qui peut être définie est fixée au 18 janvier 2038.

Indication d'une protection de données au niveau de la spécification de sauvegarde

Vous pouvez définir la protection des données lorsque vous créez une spécification de sauvegarde ou en modifiez une.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**, puis le type

de spécification approprié (par exemple **système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.

3. Cliquez deux fois sur la spécification de sauvegarde dont vous souhaitez définir les options, puis cliquez sur l'onglet **Options**.
4. Si vous sauvegardez des systèmes de fichiers, spécifiez l'option Protection sous Options du système de fichiers. Dans le cas d'intégrations, cliquez sur **Avancé** sous Options communes de l'application et spécifiez l'option **Protection** dans l'onglet Options.
5. Cliquez sur **OK** puis sur **Appliquer** pour enregistrer les modifications.

Indication d'une protection de données pour des objets sauvegarde individuels

Vous pouvez spécifier une période de protection différente pour des objets image disque et système de fichiers.

Vous pouvez définir la protection des données des différents objets lorsque vous créez une spécification de sauvegarde ou en modifiez une.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**, puis le type de spécification approprié (par exemple **système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez deux fois sur la spécification de sauvegarde dont vous souhaitez définir les options, puis cliquez sur l'onglet **Résumé d'objet sauvegarde**.
4. Cliquez avec le bouton droit de la souris sur un objet, puis cliquez sur **Propriétés**.
5. Cliquez sur l'onglet **Options** et spécifiez l'option Protection.
6. Cliquez sur **OK** puis sur **Appliquer** pour enregistrer les modifications.

Indication d'une protection de données pour des sauvegardes planifiées

Vous pouvez indiquer une période de protection différente pour chaque sauvegarde planifiée périodique ou individuelle. La protection de données indiquée dans l'assistant Planifier remplace tous les autres paramètres de protection de données dans la spécification de sauvegarde.

Vous pouvez indiquer la protection de données d'une sauvegarde planifiée lors de la planification d'une sauvegarde.

Indication d'une protection de données à l'aide de l'interface de ligne de commande

Lorsque vous exécutez une sauvegarde à l'aide de l'interface de ligne de commande, vous pouvez également définir la protection de données. Cette définition remplace tous les paramètres de protection

de données dans la spécification de sauvegarde.

Procédure

1. Entrez la commande suivante :

   ```
   omnib -datalist Name -protect ProtectionPeriod
   ```

   Où *Name* est le nom de la spécification de sauvegarde.

   Par exemple, pour exécuter une sauvegarde avec une protection de deux semaines, saisissez :

   ```
   omnib -datalist MyBackup -protect weeks 2
   ```

   Pour plus d'informations, reportez-vous à la page de manuel `omnib` ou à la *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Modification des options d'un objet spécifique

Vous pouvez appliquer des options à des objets spécifiques ou changer manuellement les options par défaut.

Vous pouvez appliquer ces options de sauvegarde lorsque vous créez une spécification de sauvegarde. Pour cela, vous devez accéder à la page Résumé d'objet sauvegarde, en suivant les indications de l'assistant.

Vous pouvez également appliquer les options de spécifications de sauvegarde déjà configurées et enregistrées.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécifications de sauvegarde**, puis le type de spécification de sauvegarde (par exemple **Système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez deux fois sur la spécification à laquelle vous souhaitez appliquer des options pour un objet spécifique, puis sélectionnez l'onglet **Résumé d'objet sauvegarde**.
4. Dans la page Résumé d'objet sauvegarde, vous pouvez modifier des propriétés d'objet, l'ordre des objets ou les options de mise en miroir.

   Pour modifier des propriétés d'objet :

   a. Cliquez avec le bouton droit de la souris sur l'objet, puis cliquez sur **Propriétés**.
   b. Dans la boîte de dialogue Propriétés d'objet, modifiez les options pour l'objet spécifique. Selon l'objet sélectionné, certains des onglets suivants sont affichés : **Général**, **Options**, **Autre**, **Arbres/Filtres**, **Options WinFS** ,**Options**, et **Base de données**. Cliquez sur l'onglet approprié pour modifier les options.
   c. Cliquez sur **OK** pour appliquer la configuration.

   Pour modifier l'ordre des objets :

   a. Cliquez avec le bouton droit de la souris sur un objet, puis choisissez **Monter** ou **Descendre**. Répétez la procédure jusqu'à ce que vous obteniez l'ordre souhaité.
   b. Cliquez sur **Appliquer**.

Pour modifier les options de mise en miroir, procédez comme suit :

a. Sélectionnez un objet et cliquez sur **Changer miroir**.
b. Pour changer de périphérique, assurez-vous que le miroir concerné est sélectionné, mettez-le en surbrillance et sélectionnez un périphérique dans la liste déroulante **Périphérique**. Vous pouvez également désélectionner un miroir pour l'objet sauvegarde sélectionné.

Modification des options du périphérique de sauvegarde

Vous pouvez définir les options du périphérique de sauvegarde et l'ordre des périphériques lorsque vous créez une spécification de sauvegarde. Ces options se définissent dans la page de propriétés Destination de l'assistant.

Vous pouvez également définir les options du périphérique de sauvegarde pour une spécification déjà configurée et enregistrée.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécifications de sauvegarde**, puis le type de spécification de sauvegarde (par exemple **Système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez deux fois sur la spécification dont vous souhaitez modifier les options de périphérique, puis sélectionnez l'onglet **Destination**.
4. Dans la page de propriétés Destination, vous pouvez modifier des options de périphérique.
   - Pour changer les périphériques d'une sauvegarde qui est en partage de charge, désélectionnez-les et choisissez-en d'autres.
   - Pour changer les périphériques d'une sauvegarde qui n'est pas en partage de charge, sélectionnez tous les périphériques que vous voulez utiliser. Ensuite, cliquez sur l'onglet **Résumé d'objet sauvegarde**, sélectionnez l'objet voulu et cliquez sur **Changer périphérique**.
   - Si vous voulez changer des périphériques pour un objet mis en miroir, sélectionnez tous les périphériques à utiliser pour un miroir spécifique. Ensuite, cliquez sur l'onglet **Résumé d'objet sauvegarde**, sélectionnez l'objet voulu et cliquez sur **Changer miroir**.
   - Pour modifier l'ordre des périphériques (si la sauvegarde est en partage de charge), cliquez avec le bouton droit de la souris sur un périphérique sélectionné et cliquez sur **Trier périphériques**.
   - Pour définir d'autres propriétés de périphérique, cliquez avec le bouton droit de la souris sur un périphérique sélectionné et choisissez **Propriétés**.
5. Indiquez les options de votre choix et cliquez sur **OK**.
6. Cliquez sur **Appliquer**.

Définition des options de planification de sauvegarde

Lors de la planification d'une sauvegarde, vous pouvez définir des options supplémentaires. Ces options ne s'appliquent qu'aux sauvegardes planifiées et non à celles qui sont lancées de manière interactive. La protection de données qui est spécifiée dans l'assistant Planifier remplace tout autre paramètre de protection dans la spécification de sauvegarde.

Vous pouvez définir des options de planification de sauvegarde lorsque vous créez une spécification de sauvegarde pour une sauvegarde planifiée. Sélectionnez l'option **Enregistrer et planifier** de l'assistant Sauvegarder pour planifier la sauvegarde.

Vous pouvez également définir des options de planification de sauvegarde lorsque vous planifiez une sauvegarde dans une spécification que vous avez déjà configurée et enregistrée. Pour plus d'informations sur la création et la modification de planifications dans Data Protector, voir *Planificateur, Page 110*.

A propos des commandes pré- et post-exécution

Que sont les commandes pré- et post-exécution ?

Les commandes pré- et post-exécution servent à réaliser des actions supplémentaires avant et après une sauvegarde ou une restauration. Ces actions comprennent la vérification du nombre de fichiers à sauvegarder, l'arrêt du traitement de certaines transactions ou la fermeture d'une application avant la sauvegarde et son redémarrage ensuite. Les commandes pré- et post-exécution ne sont pas fournies par Data Protector. Vous devez écrire vos propres scripts pour effectuer les actions souhaitées. Ils peuvent être écrits sous forme d'exécutables ou de fichiers de commandes sur des systèmes Windows, ou de scripts shell sur des systèmes UNIX. Toutes les commandes exécutées dans le fichier de commandes doivent renvoyer le code de sortie `0` en cas de réussite ou un code de sortie supérieur à `0` en cas d'échec.

Il existe un comportement spécial pour les objets sauvegarde du type `Client System` (sauvegarde de l'hôte). Même si les commandes pré- et post exécution ne sont spécifiées qu'une seule fois, chacune d'entre elles est démarrée une fois pour chaque système de fichiers (ou périphérique logique).

Configuration des commandes pré- et post-exécution pour une sauvegarde

Les commandes pré- et post-exécution peuvent être configurées sur deux niveaux :

Spécification de sauvegarde

La commande pré-exécution est exécutée avant le démarrage de la session de sauvegarde. La commande post-exécution est exécutée lorsque la session de sauvegarde s'arrête. Ces commandes doivent être spécifiées comme des options de sauvegarde pour l'ensemble de la spécification de sauvegarde. Par défaut, les commandes de pré- et post-exécution pour la session de sauvegarde sont exécutées sur le Gestionnaire de cellule, mais vous pouvez choisir un autre système.

Objet sauvegarde

La commande post-exécution pour un objet sauvegarde s'exécute après la sauvegarde de cet objet. La commande post-exécution s'exécute après la sauvegarde de cet objet. Ces commandes doivent être spécifiées comme des options de sauvegarde pour les objets. Ces deux types de commande s'exécutent sur le système où l'Agent de disque qui sauvegarde l'objet s'exécute.

Comment fonctionnent les commandes pré- et post-exécution ?

1. La commande pré-exécution pour l'ensemble de la spécification de sauvegarde se lance et s'effectue.
2. Pour chaque objet de la spécification de sauvegarde :
   a. La commande pré-exécution se lance et s'effectue.
   b. L'objet est sauvegardé.
   c. La commande post-exécution (pour chaque objet de la spécification de sauvegarde) se lance et s'effectue.
3. La commande post-exécution pour l'ensemble de la spécification de sauvegarde se lance et s'effectue.

Commandes pré- et post-exécution d'une spécification de sauvegarde

Les commandes pré- et post-exécution peuvent être écrites sous forme d'exécutables ou de fichiers de commandes sur des systèmes Windows, ou de scripts shell sur des systèmes UNIX. Toutes les commandes exécutées dans le fichier de commandes doivent renvoyer le code de sortie 0 en cas de réussite ou un code de sortie supérieur à 0 en cas d'échec.

Caractéristiques des commandes pré- et post-exécution

- Démarrage et emplacement des commandes assurant la sécurité
- Variables d'environnement
- Valeurs SMEXIT
- À propos des commandes pré- et post-exécution

Démarrage et emplacement des commandes assurant la sécurité

Les commandes pré- et post-exécution d'une session de sauvegarde sont lancées respectivement avant et après la session. Elles sont exécutées sur le Gestionnaire de cellule par défaut, mais vous pouvez choisir un autre système.

Systèmes Windows

Les scripts de pré- et de post-exécution sont lancés par Data Protector CRS quand ils s'exécutent dans le Gestionnaire de cellule, et sous le compte du service Inet Data Protector (par défaut, le compte

système local) quand ils s'exécutent à distance.

Les scripts sur le Gestionnaire de cellule et d'autres systèmes doivent être localisés dans le répertoire `Data_Protector_ home\bin` et l'utilisateur ne doit spécifier que le nom de fichier ou le chemin d'accès relatif.

Seules les extensions `.bat`, `.exe` et `.cmd` sont prises en charge pour les commandes pré- et post-exécution. Pour exécuter un script avec une extension non prise en charge (par exemple `.vbs`), créez un fichier de commandes qui démarre le script. Configurez ensuite Data Protector pour exécuter le fichier de commandes en tant que commande pré-exécution ou post-exécution, qui lance à son tour le script avec l'extension non prise en charge.

Si vous utilisez des guillemets ("") dans le chemin d'accès, n'employez pas de barre oblique inverse (\). Si vous devez placer une barre oblique inverse à la fin du chemin d'accès, doublez ce caractère (\\).

> **REMARQUE :**
> L'utilisation directe de perl.exe est interdite.

Systèmes UNIX

Les scripts de pré- et de post-exécution sont lancés par le propriétaire de la session de sauvegarde, à moins qu'il n'ait une autorisation `Backup as root`; dans ce cas, les commandes sont lancées sous `root`.

Sur le Gestionnaire de cellule ou un client UNIX distant, les commandes d'exécution pour les spécifications de sauvegarde doivent être situées comme suit :

Systèmes HP-UX, Solaris et Linux : `/opt/omni/lbin`

Autres systèmes UNIX : `/usr/omni/bin`

Pour les commandes situées dans le répertoire `/opt/omni/lbin` ou `/usr/omni/bin`, indiquez uniquement le nom de fichier. Sinon, indiquez le chemin d'accès complet.

Variables d'environnement

Les variables d'environnement suivantes sont définies avec Data Protector et peuvent être utilisées uniquement dans des scripts pré- et post-exécution pour une spécification de sauvegarde sur le Gestionnaire de cellule, sauf si la commande est exécutée sur un autre système.

Pour plus d'informations sur les variables d'environnement, reportez-vous au Aide de HPE Data Protector.

- DATALIST
- MODE
- OWNER
- PREVIEW
- RESTARTED
- SESSIONID
- SESSIONKEY
- SMEXIT

Valeurs SMEXIT

Valeur	Description
0	Tous les fichiers ont été sauvegardés avec succès.
10	Tous les agents ont terminé avec succès, mais une partie des fichiers n'a pas été sauvegardée.
11	Au moins un agent a échoué ou il existe une erreur de base de données.
12	Aucun des agents n'a effectué l'opération ; la session a été abandonnée par Data Protector.
13	La session a été abandonnée par un utilisateur.

À propos des commandes pré- et post-exécution

- Sur les systèmes Windows, vous devez spécifier le nom de fichier complet, extension comprise (par exemple `..exe` ou `.bat`).
- Lorsque vous spécifiez le nom du script, si vous êtes amené à utiliser des apostrophes (sur les systèmes UNIX) ou des guillemets (sur les systèmes Windows), du fait d'espaces dans un chemin, ne combinez jamais les deux. Utilisez au choix des apostrophes ou des guillemets. Par exemple, "S'ilvousplait.bat" est incorrect, S'ilvousplait.bat est autorisé.
- En cas de réussite, la valeur de sortie d'une commande pré- ou post-exécution doit être zéro.
- Si une commande pré-exécution échoue (renvoie une value inférieure à `0`), l'état de la session de sauvegarde est défini sur `Failed` et la session est abandonnée. Aucune commande post-exécution n'est exécutée.
- Si une commande post-exécution échoue (renvoie une valeur inférieure à `0`), l'état de la session de sauvegarde est défini sur `Completed with errors` avec des erreurs.
- Si une commande post-exécution renvoie une valeur inférieure à `0` et la commande omnib 11, l'état de la session de sauvegarde est défini sur `Completed with failures`.
- La commande post-exécution est toujours exécutée, sauf si la session est abandonnée et si la commande pré-exécution n'est pas exécutée ou définie. Si l'option omnirc `OB2FORCEPOSTEXEC` est définie, la commande post-exécution est toujours exécutée.
- Par défaut, les commandes pré- et post-exécution ne sont PAS exécutées lors du test de la sauvegarde. Ce comportement est défini par l'option `ExecScriptOnPreview` dans le fichier d'options globales.
- Les commandes pré- et post-exécution sont gérées de la même manière que les commandes saisies à l'invite de commande. Cependant, les caractères spéciaux ?, *, ", |, < et > ne sont pas autorisés.
- L'exécution des commandes pré- et post-exécution s'effectue à l'aide du mécanisme de canal de communication. Tous les processus lancés dans les fonctions pré- ou post-exécution doivent se terminer avant la suite de la procédure.
- Une session de sauvegarde ne peut pas être abandonnée lorsqu'une commande pré- ou post-

exécution est en cours.

- Les commandes pré- et post-exécution sont exécutées en arrière-plan. Vous ne devez donc pas utiliser de commande nécessitant l'interaction utilisateur.
- Il existe un délai. Les scripts de pré- et de post-exécution doivent envoyer un résultat au minimum tous les quarts d'heure (par défaut) ; sinon, ils sont abandonnés. Toutefois, vous pouvez changer ce délai en modifiant l'option globale `ScriptOutputTimeout`.
- Le résultat des commandes pré- et post-exécution est inscrit dans l'IDB (base de données interne) et affiché dans l'interface graphique Data Protector.
- Sur les systèmes UNIX, un script de pré- ou de post-exécution peut cesser de répondre lorsque tous les descripteurs de fichiers n'ont pas été fermés avant le début d'un nouveau processus. Si ce nouveau processus s'exécute en arrière-plan et qu'il ne s'arrête pas comme, par exemple, le processus du serveur de base de données (`dbstart`), les scripts cessent de répondre.

  Vous pouvez utiliser la commande `detach`. La source de la commande `detach` est fournie dans le dossier `detach.c` mais n'est pas prise en charge. Par exemple : `/opt/omni/bin/utilns/detach pre_script [arguments...]`
- Vous pouvez désactiver l'exécution des commandes pré- et post-exécution de la session sur le Gestionnaire de cellule en définissant l'option globale `SmDisableScript` sur 1.
- Vous pouvez désactiver l'exécution des commandes pré- et post-exécution de la session distante sur tout client, en ajoutant la ligne OB2REXECOFF=1 dans le fichier `omnirc`.
- Vous pouvez sécuriser le client en spécifiant les Gestionnaires de cellule autorisés à y accéder. Seuls les Gestionnaires de cellule autorisés pourront exécuter des commandes pré- et post-exécution sur le client.
- Sur les systèmes UNIX, le texte généré par une commande vers `stdout` est envoyé au Gestionnaire de session et écrit dans la base de données. `stderr` est redirigé vers `/dev/null`. Vous pouvez la rediriger vers `stdout` pour consigner les messages d'erreur dans la base de données.

Indication de commandes pré- et post-exécution pour une spécification de sauvegarde

Pour indiquer des commandes pré- et post-exécution pour une spécification de sauvegarde enregistrée, procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**, puis le type de spécification approprié (par exemple **système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez deux fois sur la spécification de sauvegarde pour laquelle vous souhaitez indiquer des commandes pré- et post-exécution, puis cliquez sur l'onglet **Options**.
4. Sous Options de spécification de sauvegarde, cliquez sur Avancé
5. Dans la boîte de dialogue Options de sauvegarde, onglet Général, entrez le nom du fichier ou le chemin d'accès dans la zone de texte Pré-exécution ou Post-exécution.
6. Cliquez sur **OK** puis sur **Appliquer** pour enregistrer les modifications.

Commandes pré- et post-exécution d'un objet sauvegarde spécifique

Les commandes pré- et post-exécution peuvent être écrites sous forme d'exécutables ou de fichiers de commandes sur des systèmes Windows et de scripts shell sur des systèmes UNIX. Toutes les commandes exécutées dans le fichier de commandes doivent renvoyer le code de sortie `0` en cas de réussite ou un code de sortie supérieur à 0 en cas d'échec.

Démarrage et emplacement des commandes

Les commandes pré- et post-exécution pour un objet sont exécutées respectivement avant et après la sauvegarde de l'objet. Vous pouvez spécifier ces commandes pour tous les objets d'une spécification de sauvegarde ou pour un objet en particulier. Lorsque vous sauvegardez des intégrations, Oracle par exemple, la base de données est considérée comme un objet, de sorte que les commandes sont exécutées avant et après la sauvegarde de la base de données. Elles sont exécutées sur le système où l'Agent de disque est exécuté.

Systèmes Windows :	Les scripts de pré- et de post-exécution d'un objet sauvegarde sont lancés sous le compte du service Inet Data Protector (par défaut, le compte système local). Les scripts d'exécution des objets sauvegarde peuvent se trouver dans n'importe quel répertoire du système sur lequel l'Agent de disque est exécuté. Cependant, pour les sauvegardes client, ils doivent se trouver dans *répertoire_Data_Protector*`\bin`. Si les scripts se trouvent dans le répertoire *répertoire_Data_Protector*`\bin`, indiquez uniquement le nom de fichier. Sinon, indiquez le chemin d'accès complet. Seules les extensions `.bat`, `.exe` et `.cmd` sont prises en charge pour les commandes pré- et post-exécution. Pour exécuter un script avec une extension non prise en charge (par exemple `.vbs`), créez un fichier de commandes qui démarre le script. Configurez ensuite Data Protector pour exécuter le fichier de commandes en tant que commande pré-exécution ou post-exécution, qui lance à son tour le script avec l'extension non prise en charge. Si vous utilisez des guillemets ("") dans le chemin d'accès, n'employez pas de barre oblique inverse (\). Si vous devez placer une barre oblique inverse à la fin du chemin d'accès, doublez ce caractère (\\).
Systèmes UNIX :	Les scripts de pré- et de post-exécution sont lancés par le propriétaire de la session de sauvegarde, à moins qu'il n'ait une autorisation `Backup as root`; dans ce cas, les commandes sont lancées sous root. Les commandes d'exécution des objets sauvegarde peuvent se trouver dans n'importe quel répertoire du système sur lequel l'Agent de disque est exécuté. Cependant, pour les sauvegardes de clients, ils doivent se trouver dans le répertoire des commandes administratives de Data Protector par défaut. Si les commandes se trouvent dans le répertoire des commandes administratives par défaut, indiquez uniquement le nom de fichier. Sinon, indiquez le chemin d'accès complet.

Variable d'environnement

Pour que la commande post-exécution Data Protector définisse la variable d'environnement BDACC.

À propos des commandes pré- et post-exécution

- Si vous effectuez la sauvegarde d'un système client (hôte), le script pré-exécution est lancé une fois, avant la première sauvegarde du système de fichiers d'un système particulier, alors que le script post-exécution est lancé lorsque la sauvegarde est terminée. Dans ce cas, `BDACC` ne peut être exportée car cette variable est liée à un objet de système de fichiers unique, et non à tout un système client (hôte).
- Sur les systèmes Windows, vous devez spécifier le nom de fichier complet, extension comprise (par exemple `..exe` ou `.bat`).
- Lorsque vous spécifiez le nom du script, si vous êtes amené à utiliser des apostrophes (sur les systèmes UNIX) ou des guillemets (sur les systèmes Windows), du fait d'espaces dans un chemin, ne combinez jamais les deux. Utilisez au choix des apostrophes ou des guillemets. Par exemple, "S'ilvousplait.bat" est incorrect, S'ilvousplait.bat est autorisé.
- En cas de réussite, la valeur de sortie d'une commande pré- ou post-exécution doit être zéro.
- Si une commande pré-exécution échoue (affiche une valeur non nulle), la sauvegarde de l'objet est abandonnée. L'état `Aborted` est attribué à l'objet ; l'Agent de disque arrête le traitement, mais la commande post-exécution est exécutée (sauf si elle dépend de la variable d'environnement `BDACC`). Il n'existe aucune sauvegarde de l'objet.
- Si une commande post-exécution échoue (affiche une valeur non nulle), l'état de l'objet est défini sur `Aborted`. L'objet a été sauvegardé et les données peuvent être restaurées.
- Si le client ne comporte aucun script exécutable ou si le chemin d'accès du script est incorrect, Data Protector affiche un message d'erreur indiquant l'échec du script et l'abandon de la session.
- Par défaut, les commandes pré- et post-exécution ne sont PAS exécutées lors du test de la sauvegarde. Ce comportement est défini par l'option globale `ExecScriptOnPreview`.
- Les commandes pré- et post-exécution sont gérées de la même manière que les commandes saisies à l'invite de commande. Cependant, les caractères spéciaux ?, *, ", |, < et > ne sont pas autorisés.
- Une session de sauvegarde ne peut pas être abandonnée lorsqu'une commande pré- ou post-exécution est en cours.
- Les processus pré- et post-exécution fonctionnent en arrière-plan. Vous ne devez donc pas utiliser de commande nécessitant l'interaction utilisateur dans les commandes pré- et post-exécution.
- Il existe un délai. Les scripts de pré- et de post-exécution doivent envoyer un résultat au minimum tous les quarts d'heure (par défaut) ; sinon, ils sont abandonnés. Toutefois, vous pouvez changer ce délai en modifiant l'option globale `ScriptOutputTimeout`.
- Le résultat des commandes pré- et post-exécution est inscrit dans l'IDB (base de données interne) et affiché dans l'interface utilisateur graphique Data Protector.
- Sur les systèmes UNIX, un script de pré- ou de post-exécution peut cesser de répondre lorsque tous les descripteurs de fichiers n'ont pas été fermés avant le début d'un nouveau processus. Si ce nouveau processus s'exécute en arrière-plan et qu'il ne s'arrête pas comme, par exemple, le processus du serveur de base de données (`dbstart`), les scripts cessent de répondre.

Vous pouvez utiliser la commande `detach`. La source de la commande `detach` est fournie dans le dossier `detach.c` mais n'est pas prise en charge. Par exemple : `/opt/omni/bin/utilns/detach pre_script [arguments...]`

- Les commandes pré- et post-exécution doivent envoyer un résultat à l'Agent de disque au moins toutes les deux heures (par défaut) ; sinon, la sauvegarde de l'objet est abandonnée. Toutefois, vous pouvez changer ce délai en modifiant l'option globale `SmDaIdleTimeout`.
- Sur les systèmes UNIX, le texte généré par une commande vers `stdout` est envoyé au Gestionnaire de session et écrit dans la base de données. `stderr` est redirigé vers `/dev/null`. Vous pouvez la rediriger vers `stdout` pour consigner les messages d'erreur dans la base de données.

A propos de la sécurité

Les commandes pré- et post-exécution sont potentiellement dangereuses car elles peuvent permettre à des personnes non autorisées d'exécuter un grand nombre d'actions. Si vous ne les utilisez pas, il est conseillé de les désactiver. De même, si vous utilisez des scripts de pré- et de post-exécution, conservez-les dans un emplacement sécurisé pour empêcher toute personne non autorisée de les modifier.

En réglant l'option globale `StrictSecurityFlag` sur `0x0100`, seuls les utilisateurs avec les permissions **Sauvegarder en tant que root** ou **Restaurer en tant que root** sont autorisés à exécuter les commandes pré-/post-exécution.

Vous pouvez désactiver les scripts pré- et post-exécution pour un objet sauvegarde quelconque en ajoutant la ligne `OB2OEXECOFF=1` dans le fichier `omnirc` sur le client concerné. Pour désactiver l'exécution des commandes pré- et post-exécution de la session distante sur tout client, ajoutez `OB2REXECOFF=1` dans le fichier `omnirc` sur le client.

Vous pouvez sécuriser le client en spécifiant les Gestionnaires de cellule autorisés à y accéder. Seuls les Gestionnaires de cellule autorisés pourront exécuter des commandes pré- et post-exécution sur le client.

Indication de commandes pré- et post-exécution pour des objets sauvegarde

Indication de commandes pré- et post-exécution pour tous les objets

Pour indiquer des commandes pré- et post-exécution pour tous les objets d'une spécification de sauvegarde enregistrée, procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**, puis le type de spécification approprié (par exemple **système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez deux fois sur la spécification de sauvegarde pour laquelle vous souhaitez indiquer des commandes pré- et post-exécution, puis cliquez sur l'onglet **Options**.
4. Sous Options du système de fichiers (Options d'image disque dans une spécification de

sauvegarde enregistrée pour la sauvegarde d'une image disque), cliquez sur **Avancé**.

5. Dans la boîte de dialogue Options du système de fichiers (Options d'image disque pour la sauvegarde d'une image disque), dans l'onglet Options, saisissez le nom de fichier ou le chemin d'accès dans la zone de texte **Pré-exécution** et/ou **Post-exécution**.
6. Cliquez sur **OK** puis sur **Appliquer** pour enregistrer les modifications.

Indication de commandes pré- et post-exécution pour des objets individuels

Pour indiquer des commandes pré- et post-exécution uniquement pour certains objets d'une spécification de sauvegarde enregistrée, procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez l'élément **Spécifications de sauvegarde**, puis le type de spécification approprié (par exemple **système de fichiers**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez deux fois sur la spécification de sauvegarde pour laquelle vous souhaitez indiquer des commandes pré- et post-exécution, puis cliquez sur l'onglet **Résumé d'objet sauvegarde**.
4. Cliquez avec le bouton droit de la souris sur un objet, puis cliquez sur **Propriétés**.
5. Dans la boîte de dialogue Propriétés d'objet, cliquez sur l'onglet **Options**.
6. Saisissez le nom de fichier ou le chemin d'accès dans la zone de texte **Pré-exécution** et/ou **Post-exécution**.
7. Cliquez sur **OK** puis sur **Appliquer** pour enregistrer les modifications.

Indication de commandes pré- et post-exécution pour des intégrations

Lorsque vous sauvegardez des intégrations, Oracle par exemple, la base de données est considérée comme un objet, de sorte que les commandes sont exécutées avant et après la sauvegarde de la base de données. Les commandes sont exécutées sur le client de l'application.

Pour indiquer des commandes pré- et post-exécution pour une intégration d'une spécification de sauvegarde enregistrée, procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis le type de spécification de sauvegarde approprié (par exemple, **Serveur Oracle**). Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez deux fois sur la spécification de sauvegarde pour laquelle vous souhaitez indiquer des commandes pré- et post-exécution, puis cliquez sur l'onglet **Options**.
4. Sous Options spécifiques de l'application, cliquez sur **Avancé**.
5. Dans la boîte de dialogue Options spécifiques de l'application, saisissez le nom de fichier ou le chemin d'accès dans la zone de texte **Pré-exécution** et/ou **Post-exécution**.
6. Cliquez sur **OK** puis sur **Appliquer** pour enregistrer les modifications.

A propos de la planification de sauvegarde

> **IMPORTANT :**
> Avec Data Protector 10.00, les planificateur de base et avancé sont rendus obsolètes et remplacés par un nouveau planificateur Web. Pendant la mise à niveau de Data Protector, toutes les planifications Data Protector existantes sont automatiquement migrées vers le nouveau planificateur.

Vous pouvez configurer des sauvegardes sans surveillance en planifiant des sessions de sauvegarde à exécuter à des instants précis. Les planifications peuvent être définies à des intervalles quotidiens, hebdomadaires ou mensuels. En outre, vous pouvez également spécifier les options de planification, telles que la priorité, la charge de réseau et la protection des données.

Pour plus d'informations sur la création et la modification de planifications dans Data Protector, voir *Planificateur, Page 110*.

Exécution de sauvegardes consécutives

Vous pouvez démarrer une sauvegarde dès que la précédente est terminée. Par exemple, vous pouvez démarrer une sauvegarde de la base de données Oracle dès que celle du système de fichiers est terminée.

Utilisez la commande post-exécution dans la première spécification de sauvegarde pour démarrer une sauvegarde consécutive.

Procédure

1. Planifiez la première sauvegarde.
2. Cliquez sur l'onglet Options, puis sur Avancé sous Options de spécification de sauvegarde.
3. Dans la zone de texte Post-exécution, saisissez la commande `omnib` avec le nom de la spécification de sauvegarde à démarrer une fois que la première est terminée (par exemple, `omnib -datalist` *`name_of_the_backup_specification`*), puis cliquez sur **OK**.

> **CONSEIL :**
> Vous pouvez également spécifier votre propre script pour vérifier l'état de la première sauvegarde.

À propos des groupes de spécifications de sauvegarde

Data Protector vous permet d'organiser les spécifications de sauvegarde en différents groupes. Ceci est pratique si, par exemple, vous devez gérer un grand nombre de spécifications de sauvegarde et que vous souhaitez les regrouper en fonction de caractéristiques communes.

Un regroupement significatif permet de faciliter la recherche et la gestion des différentes spécifications de sauvegarde. Ceci permet également d'appliquer à l'ensemble du groupe des paramètres d'option communs provenant d'un modèle. Par exemple, si vous souhaitez modifier la liste des périphériques

pour toutes les spécifications de sauvegarde du groupe, vous pouvez appliquer de manière sélective les paramètres de périphérique d'un modèle.

CONSEIL :
Vous pouvez appliquer à un groupe de spécifications de sauvegarde des paramètres d'options courants (pour les périphériques par exemple) provenant d'un modèle. Pour cela, sélectionnez toutes les spécifications du groupe (cliquez sur le nom du groupe, puis appuyez sur CTRL+A), puis cliquez avec le bouton droit sur un groupe cible. Choisissez ensuite **Appliquer modèle**.

REMARQUE :
L'interface utilisateur graphique Data Protector permet d'afficher un nombre limité de spécifications de sauvegarde. Le nombre de spécifications de sauvegarde dépend de la taille de leurs paramètres (informations sur le nom, le groupe, la propriété et le partage de charge ou non). Cette taille ne doit pas dépasser 80 Ko.

Exemple de groupes de spécifications de sauvegarde

Les spécifications de sauvegarde d'une société importante peuvent être regroupées de la façon suivante :

User_files	Ce groupe contient les spécifications de sauvegarde qui effectuent des sauvegardes complètes de façon hebdomadaire pour tous les utilisateurs de chacun des dix départements de la société.
SERVERS_DR	Ce groupe contient les spécifications de sauvegarde des serveurs de la société permettant de préparer la récupération après sinistre. Chaque fois qu'un nouveau serveur est installé, une spécification de sauvegarde est créée et ajoutée à ce groupe.
END_USER_ ARCHIVE	Ce groupe contient les spécifications de sauvegarde effectuées pour chaque requête émise par un utilisateur final. Par exemple, un utilisateur souhaitant libérer de l'espace sur son disque doit d'abord archiver ses disques durs.

Affichage des groupes de spécifications de sauvegarde

Dans les procédures Data Protector, il est supposé que vous utilisez l'affichage de sauvegarde défini par défaut (Par type). Vous pouvez modifier l'affichage pour voir les spécifications de sauvegarde arrangées par groupes.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans le menu Affichage, sélectionnez Par groupe.

Création d'un groupe de spécifications de sauvegarde

Vous pouvez créer différents groupes de spécifications de sauvegarde en utilisant plusieurs critères.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans le menu Affichage, cliquez sur **Par groupe**. La liste des groupes de sauvegardes disponibles s'affiche sous Spécification de sauvegarde dans la fenêtre de navigation.
3. Cliquez avec le bouton droit sur l'élément **Spécification de sauvegarde**, puis cliquez sur **Ajouter groupe**. La boîte de dialogue Ajouter nouveau groupe s'affiche alors.
4. Dans la zone de texte Nom, saisissez un nom pour le nouveau groupe, puis cliquez sur OK.

Le nouveau groupe de spécifications de sauvegarde s'affiche sous l'élément Spécification de sauvegarde. Vous pouvez alors ajouter des spécifications aux groupes appropriés.

Enregistrement d'une spécification de sauvegarde dans un groupe

Vous pouvez enregistrer une nouvelle spécification de sauvegarde dans un groupe spécifique.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans le menu Affichage, cliquez sur **Par groupe**. La liste des groupes de sauvegardes disponibles s'affiche sous Spécifications de sauvegarde dans la fenêtre de navigation.
3. Développez Spécifications de sauvegarde, cliquez avec le bouton droit sur le groupe auquel vous souhaitez ajouter une spécification de sauvegarde, puis cliquez sur Ajouter sauvegarde pour ouvrir l'assistant Sauvegarde.
4. Suivez les indications de l'assistant pour créer une spécification de sauvegarde. Dans la dernière page (page Enregistrer, Démarrer ou Tester) de l'assistant, cliquez sur **Enregistrer sous**. La boîte de dialogue correspondante s'affiche alors.
5. Dans la zone de texte Nom, saisissez le nom de la spécification de sauvegarde.
6. Dans la liste déroulante Groupe, sélectionnez le groupe dans lequel vous souhaitez enregistrer la spécification, puis cliquez sur **OK** pour enregistrer la spécification et quitter l'assistant. Par défaut, le groupe de sauvegardes affiché est celui que vous avez sélectionné pour lancer l'assistant.

La spécification de sauvegarde enregistrée s'affiche sous le groupe sélectionné.

Déplacement de spécifications de sauvegarde ou de modèles entre groupes

Vous pouvez déplacer une spécification de sauvegarde ou un modèle d'un groupe de sauvegardes à l'autre.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans le menu Affichage, cliquez sur **Par groupe**. La liste des groupes de sauvegardes disponibles s'affiche sous Spécifications de sauvegarde et Modèles dans la fenêtre de navigation.
3. Développez Spécifications de sauvegarde ou Modèles et le groupe contenant la spécification de sauvegarde ou le modèle que vous souhaitez déplacer.
4. Cliquez avec le bouton droit sur la spécification de sauvegarde ou le modèle à déplacer, puis cliquez sur **Changer groupe**. La boîte de dialogue correspondante s'affiche.

   Changer groupe est désactivé si les propriétés de la spécification de sauvegarde s'affichent.
5. Dans la liste déroulante Nom, sélectionnez le groupe vers lequel vous souhaitez déplacer la spécification ou le modèle, puis cliquez sur OK.

La spécification de sauvegarde ou le modèle s'affiche sous son nouveau groupe.

Suppression d'un groupe de spécifications de sauvegarde

Vous pouvez supprimer un groupe de spécifications de sauvegarde dont vous n'avez plus besoin.

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans le menu Affichage, cliquez sur **Par groupe**.
3. Développez l'élément **Spécification de sauvegarde** et l'élément **Modèles**. La liste des groupes de sauvegardes disponibles s'affiche.
4. Développez le groupe à supprimer.

   > **IMPORTANT :**
   > Un groupe contenant des spécifications de sauvegarde et des modèles ne peut pas être supprimé. Vous devez commencer par supprimer ou déplacer les spécifications et les modèles du groupe.
5. Cliquez avec le bouton droit sur le groupe cible, puis cliquez sur **Supprimer groupe**.

Le groupe de spécifications de sauvegarde cible est alors supprimé.

A propos de la sauvegarde des systèmes Windows

La procédure de sauvegarde est identique à la procédure de sauvegarde standard, mais elle comporte certains aspects spécifiques à Windows.

Limite

Pour effectuer une sauvegarde VSS d'un système de fichiers, votre système doit comporter au moins un système de fichiers NTFS.

Eléments sauvegardés

Une sauvegarde du système de fichiers d'un disque implique la lecture de la structure de répertoires, du contenu des fichiers sur le disque sélectionné, ainsi que des informations spécifiques à Windows relatives aux fichiers et répertoires.

Windows Server 2012

- Les fichiers compressés sont sauvegardés et restaurés sous forme compressée
- Les fichiers cryptés sont sauvegardés et restaurés sous forme cryptée.

Informations spécifiques à Windows

- Noms de fichier complets au format Unicode
- Attributs FAT16, FAT32, VFAT et NTFS

  Lorsqu'un fichier a été sauvegardé, son attribut archive est désactivé. Vous pouvez modifier ce comportement en définissant l'option Ne pas utiliser l'attribut archive dans les options avancées de sauvegarde de système de fichiers de la spécification de sauvegarde.
- Flux de données autres que NTFS
- Données de sécurité NTFS
- Informations de partage des répertoires

  Si un répertoire est partagé sur un réseau, les informations de partage seront sauvegardées par défaut. Au cours de la restauration, les informations de partage seront restaurées par défaut et le répertoire sera partagé sur le réseau après la restauration. Vous pouvez modifier ce comportement en désactivant l'option **Sauvegarder les informations de partage des répertoires** .

Quels sont les éléments qui ne sont pas sauvegardés ?

Dans la spécification de sauvegarde, vous pouvez spécifier la liste des fichiers à exclure ou à ignorer par la sauvegarde (liste d'exclusion privée). Outre la liste d'exclusion privée, Data Protector exclut par défaut les éléments suivants :

Windows Vista, Windows 7, Windows 8, Windows Server 2008 et Windows Server 2012 :

- Le répertoire par défaut des fichiers journaux Data Protector d'une sauvegarde d'un client Windows Windows ou Gestionnaire de cellule (Windows Server 2008 uniquement).
- Le répertoire par défaut des fichiers temporaires Data Protector d'une sauvegarde d'un client Windows Windows ou Gestionnaire de cellule (Windows Server 2008 uniquement).
- Le répertoire de la base de données interne d'une sauvegarde de Gestionnaire de cellule Windows (Windows Server 2008 uniquement).
- Fichiers spécifiés dans la clé de registre `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`.

Windows Server 2012

- Les volumes formatés à l'aide de Resilient File System (ReFS)

Autres systèmes Windows

- Le répertoire par défaut des fichiers journaux Data Protector d'une sauvegarde de client Windows.
- Le répertoire par défaut des fichiers temporaires Data Protector d'une sauvegarde de client Windows.
- Fichiers spécifiés dans la clé de registre `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`.

Par exemple, le répertoire de la base de données interne est exclu de la sauvegarde du Gestionnaire de cellule, même s'il avait été sélectionné dans la spécification de sauvegarde. Cela est dû au fait que l'IDB doit être sauvegardée d'une manière spéciale pour garantir la cohérence des données.

Tous les hôtes Data Protector gardent leurs certificats et leurs fichiers de clé privée au lieu suivant :

- `<programdata>/Omniback/Config/sscertificates` (sur Windows)
- `/etc/opt/omni/config/sscertificates/` (sur Linux)

Pendant la sauvegarde de système de fichiers, si les fichiers sont inclus depuis le lieu susmentionné, tous les fichiers sont alors sauvegardés à part ceux contenus dans la clé privée.

Caractéristiques du système de fichiers NTFS 3.1

- Le système de fichiers NTFS 3.1 prend en charge les points d'analyse.

  Les points de montage de volume, le support de stockage unique (SIS) et les jonctions de répertoires se basent sur le concept des points d'analyse. Ces points sont sélectionnés comme tout autre objet de système de fichiers.
- Le système de fichiers NTFS 3.1 prend en charge les liens symboliques, qui sont une nouvelle fonction des systèmes d'exploitation Windows Vista et Windows Server 2008.

  Data Protector gère les liens symboliques de la même manière que les points d'analyse NTFS.
- Le système de fichiers NTFS 3.1 prend en charge les fichiers épars, ce qui permet de réduire efficacement la quantité d'espace disque allouée.

  Ces fichiers sont sauvegardés de manière éparse afin d'économiser de la place sur les bandes. Les fichiers épars sont sauvegardés et restaurés de manière éparse uniquement sur le système de fichiers NTFS 3.1.
- Certaines fonctions spécifiques au système de fichiers NTFS 3.1 sont contrôlées par les services du système qui maintiennent leurs propres enregistrements de données. Ces structures de données sont sauvegardées en tant que partie d'une sauvegarde CONFIGURATION.
- Le système de fichiers NTFS 3.1 prend en charge les ID d'objet sauvegardés par Data Protector avec d'autres flux de données.
- Fichiers cryptés

  Les fichiers NTFS 3.1 cryptés via des applications Microsoft sont sauvegardés et restaurés cryptés, mais leur contenu ne peut être correctement affiché qu'après décryptage.

Points d'analyse

Les points d'analyse sont des objets simples du système de fichiers associés à une étiquette unique appelée ID de point d'analyse. Les répertoires ou fichiers NTFS 3.1 peuvent contenir un point d'analyse, qui imite généralement le contenu en pointant vers les données d'un autre emplacement.

Par défaut, quand Data Protector rencontre des points d'analyse, les ID de points d'analyse ne sont pas suivis. Cette opération est également connue sous le terme de sauvegarde des points d'analyse bruts. Elle affecte la façon dont vous configurez vos sauvegardes :

- Si vous configurez une sauvegarde à l'aide d'une restitution de disque, toutes les données seront sauvegardées une fois.
- Si vous sauvegardez des systèmes de fichiers ou des disques contenant des points d'analyse, vous devez vous assurer que les données désignées par les points d'analyse sont sauvegardées. Par exemple, les points d'analyse de jonctions de répertoires Windows ne sont pas suivis, de sorte que les jonctions doivent être sauvegardées séparément. Les points d'analyse SIS constituent des exceptions.

  Le service de support de stockage unique (Single Instance Storage ou SIS) vérifie régulièrement les fichiers sur un disque. Si le service détecte plusieurs fichiers identiques, il les remplace par des points d'analyse et stocke les données dans un référentiel commun, réduisant ainsi l'espace disque utilisé.

Les points d'analyse vous permettent de monter des volumes logiques comme lecteurs de disques. Data Protector traite les volumes montés comme s'il s'agissait de disques ordinaires, de sorte qu'ils apparaissent comme des objets sélectionnables pour la sauvegarde.

Fichiers épars

Les fichiers épars contiennent de nombreux jeux de données nulles, beaucoup plus, par exemple, que les fichiers compressés. Lors de la sauvegarde, Data Protector ignore automatiquement les parties nulles de sorte que l'espace de support sur le périphérique de sauvegarde est alloué uniquement aux parties non nulles.

Les fichiers épars UNIX et Windows ne sont pas compatibles.

Avertissements lors de la sauvegarde de disques système

Certains fichiers du disque système sont toujours occupés et ne peuvent être ouverts par aucune application, y compris l'Agent de disque. Le contenu de ces fichiers ne peut être sauvegardé qu'en tant que partie d'une sauvegarde CONFIGURATION.

Lorsque ces fichiers sont sélectionnés par une sauvegarde de système de fichiers, par exemple lorsque l'ensemble du disque système est sauvegardé, Data Protector ne peut pas les ouvrir et génère des avertissements ou des erreurs.

Bien que ce comportement soit correct du point de vue de la sauvegarde d'un système de fichiers, il risque de compliquer la gestion. En raison du grand nombre d'avertissements qui sont toujours signalés, il se peut que la défaillance d'un autre fichier passe inaperçue.

Excluez les fichiers sauvegardés via une sauvegarde de CONFIGURATION d'une sauvegarde de système de fichiers pour éviter ces avertissements.

> **REMARQUE :**
> Lors de la sauvegarde d'un disque système inactif (par exemple dans une situation de double amorçage) les fichiers susmentionnés ne font pas partie de la sauvegarde CONFIGURATION active. Ces fichiers peuvent être sauvegardés dans une sauvegarde du système de fichiers, et ne devraient pas être exclus.

Sauvegarde de configuration (Windows)

Les structures de données particulières, maintenues par le système d'exploitation Windows, ne sont pas traitées comme une partie de la sauvegarde d'un système de fichiers. Data Protector permet de sauvegarder une structure de données particulière appelée CONFIGURATION.

Pour effectuer une sauvegarde de la configuration, sélectionnez l'objet CONFIGURATION ou simplement des parties de celui-ci lorsque vous créez une spécification de sauvegarde de système de fichiers. Les journaux d'événements, les profils et les quotas de disque utilisateur sont toujours sauvegardés si la CONFIGURATION est sélectionnée dans l'assistant de sauvegarde.

Sur les systèmes Windows Vista, Windows 7, Windows 8, Windows Server 2008 et Windows Server 2012, la sauvegarde de la CONFIGURATION est exécutée via Microsoft Volume Shadow Copy Service.

Limites

- Il n'est possible d'exécuter qu'une seule sauvegarde de CONFIGURATION à la fois sur un système.
- Le service Active Directory et SysVol doivent être sauvegardés ensemble.

Objets de configuration Windows

- Service Active Directory
- Certificate Server
- Base de données d'enregistrement des classes COM+ (`ComPlusDatabase`)
- DFS
- DHCP
- Serveur DNS
- partition d'utilitaire EISA
- Journaux d'événements
- Service de réplication de fichiers
- Internet Information Server (IIS)
- Profils utilisateur (`Documents and Settings`)
- Registre Windows
- Base de données du gestionnaire de supports amovibles
- SystemRecoveryData
- SysVol

- Base de données des services Terminal Server
- Quotas de disque utilisateur (`QuotaInformation`)
- serveur WINS

La CONFIGURATION est différente selon les systèmes Windows utilisés.

Pour certains objets, des points spéciaux doivent être pris en compte. Ils sont répertoriés dans les sections ci-dessous.

Active Directory

Lors de la sauvegarde du service Active Directory, le service de réplication des fichiers (FRS) et le système de fichiers distribués (DFS) sont également sauvegardés. Toutes les informations de configuration sur les fichiers répliqués et les fichiers distribués sont stockées dans Active Directory.

DFS

Data Protector sauvegarde le système de fichiers distribués (DFS) Windows en même temps que l'un des éléments suivants :

- Registre Windows, si le DFS est configuré en mode autonome
- Windows Active Directory, si le DFS est configuré en mode de domaine

DHCP et WINS

Lorsque Data Protector sauvegarde une base de données DHCP ou WINS, le service correspondant est arrêté, puis relancé une fois la base de données sauvegardée. Il est recommandé de planifier la sauvegarde de la CONFIGURATION d'un serveur qui exécute un service DHCP et/ou WINS en dehors des heures de travail.

Les services DHCP et WINS fournissent également leurs propres copies de sauvegarde interne de leurs bases de données. Si votre environnement ne peut pas tolérer l'arrêt occasionnel de ces services, vous pouvez les exclure des sauvegardes de la CONFIGURATION Data Protector et sauvegarder la copie de sauvegarde interne des bases de données via la sauvegarde du système de fichiers. Reportez-vous à la documentation Microsoft MSDN pour connaître l'emplacement des copies de sauvegarde interne et vous assurer que ces copies sont créées régulièrement.

Profilage

Si vous avez sélectionné la totalité du système pour la sauvegarde, "Profils" est sauvegardé deux fois (une fois dans le cadre de la sauvegarde du système de fichiers et une fois en tant que partie de CONFIGURATION). Pour éviter cela, excluez les données de profil de la sauvegarde du système de fichiers. Les données des profils utilisateur se trouvent dans le répertoire `c:\Documents and Settings`.

Ces répertoires contiennent tous les profils utilisateur configurés sur le système et sont sauvegardés par Data Protector. Si un système est configuré pour plusieurs utilisateurs, un profil différent est affecté à chacun. Par exemple, les profils `All Users` et `Default User` contiennent les composants de profil communs à tous les utilisateurs définis ainsi que les composants de profil attribués à un nouvel utilisateur.

Data Protector lit l'emplacement des profils à partir des clés de registre suivantes :

```
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\\
CurrentVersion\Explorer\Shell Folders
```

(dans lesquelles se trouvent les informations sur les composants de profil communs)

```
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\\
CurrentVersion\Explorer\User Shell Folders
```

Base de données du gestionnaire de supports amovibles

Pour permettre la sauvegarde de l'objet de configuration Base de données du gestionnaire de supports amovibles sur les systèmes d'exploitation Windows Vista et Windows Server 2008, assurez-vous que le service Gestionnaire de supports amovibles est installé sur le système à sauvegarder.

Base de données des services Terminal Server

Pour permettre la sauvegarde de l'objet de configuration Base de données des services Terminal Server sur les systèmes d'exploitation Windows Vista et Windows Server 2008, assurez-vous que le service Terminal Server Licensing est installé sur le système à sauvegarder.

Services Windows

Sauvegarder les services Windows revient à sauvegarder les structures de données utilisées par les différents services. Une base de données particulière est ainsi exportée (vidée) dans un fichier qui est ensuite sauvegardé. Les services Windows sont toujours sauvegardés si la CONFIGURATION est sélectionnée dans l'assistant de sauvegarde.

Un service Windows doit être actif pour que Data Protector puisse le détecter et le présenter comme un élément sélectionnable dans l'assistant de sauvegarde. Lorsqu'un service n'est pas actif au moment de la sauvegarde, l'objet sauvegarde correspondant échoue.

Pour sauvegarder l'un des services, sélectionnez le dossier correspondant sous CONFIGURATION. Si vous utilisez Active Directory pour publier, par exemple, des listes de résiliation de certificats (CRL), sauvegardez les services Active Directory en même temps que Certificate Server.

Sauvegarde des données d'état du système

L'état du système Windows correspond à plusieurs éléments en relation avec différents aspects du système Windows. Ces éléments sont structurés sous l'objet sauvegarde Windows correspondant.

L'état du système Windows n'est pas un élément de sauvegarde sélectionnable. Data Protector vous permet de sauvegarder des objets individuels tels que le Registre ou la Base de données d'enregistrement des classes COM+. Il est recommandé de sauvegarder l'ensemble de l'arborescence CONFIGURATION. Sur les systèmes Windows Vista, Windows 7, Windows 8, Windows Server 2008 et Windows Server 2012, la sauvegarde de volumes spécifiques ou de tout le système client à l'aide de la fonction de sauvegarde du système de fichiers avec l'option **Utiliser Shadow Copy** sélectionnée est nécessaire.

L'état du système englobe notamment les éléments suivants :

- Fichiers de démarrage : `Ntldr.exe`, `Ntdetect.com` et `boot.ini`
- `Registry` and `COM+ Class Registration Database (ComPlusDatabase)`
- `System File Protection` service conservés dans le répertoire `System Volume Information`

En outre, si les services sont installés et configurés, les données sur l'état du système d'un serveur Windows sont les suivantes :

- `ActiveDirectoryService`
- `CertificateServer`
- `Cluster Service information`
- `IIS Metadirectory`
- `RemoteStorageService`
- `RemovableStorageManagementDatabase`
- `SystemFileProtection`
- `SYSVOL directory`
- `TerminalServiceDatabase`

Sur les systèmes Windows Vista, Windows 7, Windows 8, Windows Server 2008 et Windows Server 2012, les données d'état du système incluent également des données appartenant à d'autres services ou rôles de serveur susceptibles d'être installés.

Service de stockage distant (RSS - Remote Storage Service)

Le service de stockage distant permet de déplacer automatiquement les fichiers peu utilisés de l'emplacement de stockage local à l'emplacement de stockage distant. Les fichiers distants sont rappelés automatiquement à leur ouverture. Bien que les bases de données RSS fassent partie des données d'état du système, vous pouvez les sauvegarder manuellement.

Services de stockage distant :

- Moteur de stockage distant : *%SystemRoot%*`\system32\RsEng.exe`

  Coordonne les services et les outils d'administration utilisés pour le stockage des données rarement sollicitées.
- Fichier de stockage distant : *%SystemRoot%*`\system32\RsFsa.exe`

  Gère les opérations sur les fichiers stockés à distance.
- Notification de stockage distant : *%SystemRoot%*`\system32\RsNotify.exe`

  Envoie au client une notification relative aux données rappelées.

Bases de données de stockage distant :

Les bases de données de stockage distant se trouvent dans le répertoire suivant : *%SystemRoot%*`\system32\RemoteStorage`

- Base de données du moteur SSD : *%SystemRoot%*`\system32\RemoteStorage\EngDb`
- Base de données de sauvegarde du moteur SSD : *%SystemRoot%*`\system32\RemoteSorage\EngDb.bak`

- Base de données du fichier SSD : *%SystemRoot%*\system32\RemoteStorage\FsaDb
- Base de données de trace SSD : *%SystemRoot%*\system32\RemoteStorage\Trace

Base de données du gestionnaire de supports amovibles

Vous pouvez sauvegarder la base de données du gestionnaire de supports amovibles, mais ce service n'est pas utilisé pour la gestion des supports Data Protector. Il faut désactiver le pilote de robots d'origine utilisé pour les changeurs de supports robotiques avant que Data Protector ne configure un périphérique.

Protection de fichiers système

Le service de protection des fichiers système analyse et vérifie les versions de tous les fichiers système protégés après le redémarrage de votre ordinateur. Si le service de protection des fichiers système découvre qu'un fichier protégé a été écrasé, il récupère la version correcte de celui-ci et remplace le fichier incorrect. Data Protector permet de sauvegarder, puis de restaurer des fichiers protégés sans les écraser. Vous pouvez sauvegarder les fichiers protégés à l'aide de l'option Déplacer fichiers occupés lors d'une procédure standard de sauvegarde de système de fichiers.

A propos de la sauvegarde des systèmes UNIX

Pour effectuer une sauvegarde sur un système UNIX, utilisez la procédure de sauvegarde standard. Vous devez effectuer quelques étapes supplémentaires lors de la sauvegarde de disques avec NFS, pour la sauvegarde d'un snapshot VxFS ou pour la sauvegarde d'une image disque UNIX.

Limites

- Lors de la sauvegarde de systèmes de fichiers montés avec NFS, les attributs de fichiers ne sont pas tous conservés.
- La taille maximale des fichiers que vous pouvez sauvegarder dépend du système d'exploitation et des limitations du système de fichiers.

Pour une liste complète des plates-formes prises en charge et des limitations connues, reportez-vous au *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*.

Eléments sauvegardés

- Data Protector sauvegarde la structure de répertoires, les fichiers normaux et les fichiers spéciaux. Les fichiers spéciaux sont des fichiers de caractères, des fichiers de blocs, des sockets de domaine UNIX, des fichiers FIFO, des fichiers spéciaux de réseau HP-UX et des fichiers spéciaux XENIX nommés.
- Les liens symboliques ne sont pas suivis et sont sauvegardés en tant que liens symboliques.
- Les points de montage ne sont pas suivis et sont sauvegardés en tant que répertoires vides ordinaires.
- Si plusieurs liens réels référant le même fichier, ce fichier n'est sauvegardé qu'une seule fois. Vous pouvez modifier cette règle en définissant l'option **Sauvegarder les liens réels POSIX en tant que**

fichiers.

- Les ACL de base (attributs d'autorisation d'accès aux fichiers) et les attributs de temps sont sauvegardés avec les fichiers sur toutes les plates-formes UNIX prises en charge. Cependant, la prise en charge des ACL étendus est limitée sur certaines plates-formes. Pour plus de détails, voir la *Matrice de prise en charge de l'intégration de HPE Data Protector* du https://softwaresupport.hpe.com/. L'heure du dernier accès à chaque fichier est enregistrée avant la lecture du fichier puis retrouve sa valeur d'origine une fois le fichier sauvegardé. Ce comportement peut être modifié en définissant l'option **Ne pas conserver les attributs de temps d'accès**.

Quels éléments devraient être exclus d'une sauvegarde de système de fichiers UNIX ?

- Les répertoires de bases de données internes, qui doivent être sauvegardés (en ligne) d'une manière spéciale ;
- Les répertoires temporaires.

Sauvegarde NFS

NFS (Network Filesystem) est un protocole de système de fichiers distribué qui permet à un ordinateur d'accéder à des fichiers sur un réseau comme s'ils étaient sur ses disques locaux. Avec NFS, vous pouvez sauvegarder un système de fichiers à partir d'un système UNIX distant accessible localement.

Quand faut-il utiliser une sauvegarde NFS ?

- Si un système ne fait pas partie de la cellule Data Protector ou ne dispose pas d'un Agent de disque.
- Lorsque vous souhaitez sauvegarder des plates-formes du système qui ne sont pas prises en charge par Data Protector.

Lorsque vous configurez une sauvegarde de système de fichiers normale, il est recommandé d'exclure de celle-ci les systèmes de fichiers montés NFS. Cela évite les messages d'avertissement et la sauvegarde dupliquée des mêmes disques, si le système sur lequel se trouvent les disques est également sauvegardé.

Limites

- Vous pouvez sauvegarder des volumes NFS montés sur des clients HP-UX, Solaris et Linux. Vous ne pouvez sauvegarder ni les liens programmables, ni les fichiers spéciaux de caractères, ni les fichiers de périphérique. Pour plus de détails sur les plates-formes prises en charge, consultez les dernières matrices de support à l'adresse https://softwaresupport.hpe.com/.
- Les attributs ACL (Access Control List) ne sont pas conservés. NFS ne prend pas en charge les ACL des fichiers distants. Les entrées manuelles individuelles permettent de spécifier le comportement de différents appels système, appels de bibliothèque et commandes. Lors du transfert d'un fichier avec des entrées facultatives sur le réseau ou lors de la manipulation d'un fichier distant, de telles entrées peuvent être supprimées sans avertissement.

La procédure de sauvegarde pour un système de fichier HP OpenVMS est la même que la procédure de sauvegarde du système de fichier classique avec certains aspects spécifiques à OpenVMS.

Conditions préalables

- Pour sauvegarder les données sur un système OpenVMS, installez l'Agent de disque OpenVMS sur le système OpenVMS.
- Pour utiliser des périphériques de sauvegarde connectés à un système OpenVMS avec Data Protector, installez l'Agent de support général sur le système OpenVMS.

Limites

- Les spécifications de fichiers saisies dans l'interface graphique ou transmises à l'interface de ligne de commande doivent respecter la syntaxe de style UNIX

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

  La chaîne doit commencer par une barre oblique, suivie par le disque, les répertoires et le nom du fichier, séparés par des barres obliques.

  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. Par exemple, une spécification de fichier OpenVMS :

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

  doit être spécifiée sous la forme :

  `/$1$DGA100/USERS/DOE/LOGIN.COM.1`
- Il n'y a pas de numéro de version implicite. Vous devez toujours spécifier un numéro de version. Seules les versions de fichier sélectionnées pour la sauvegarde seront sauvegardées. Si vous souhaitez inclure toutes les versions du fichier, sélectionnez-les toutes dans la fenêtre de l'interface graphique, ajoutez les spécifications de fichier sous l'option **Uniquement** (`-only`) en intégrant des caractères génériques pour le numéro de version, comme suit :

  `/DKA1/dir1/filename.txt.*`
- Pour sauvegarder avec succès les disques protégés et fantômes, activez l'option **Ne pas préserver les attributs temporels d'accès** dans la spécification de sauvegarde.
- Si l'option **Ne pas conserver les attributs de temps d'accès** est activée lors d'une sauvegarde, la dernière date d'accès sera mise à jour avec la date et l'heure actuelle sur les disques ODS-5. Sur les disques ODS-2, cette option n'a aucun effet et toutes les dates restent inchangées.
- Les sauvegardes d'image disque ne sont pas disponibles sur OpenVMS. Il n'y a pas d'équivalent à une sauvegarde "BACKUP/PHYSICAL".
- Les options **Sauvegarder les liens matériels de POSIX comme fichiers** (`-hlink`), **Compression du logiciel** (`-compress`) et**Encoder** (`-encode`) ne sont pas disponibles sur OpenVMS.

  Les fichiers dotés de multiples entrées de répertoire ne sont sauvegardés qu'une fois en utilisant le nom de chemin d'accès principal. Les entrées de chemin secondaire sont enregistrées en tant que

liens symboliques. Lors d'une restauration, ces entrées de chemin supplémentaires seront aussi restaurées.

Il n'y a aucune prise en charge d'une sauvegarde BACKUP/IMAGE. Pour créer une copie restaurée d'un disque système amorçable OpenVMS, l'utilitaire OpenVMS WRITEBOOT doit être utilisé pour inscrire un bloc d'amorçage sur le disque restauré.

- Les fichiers étant sauvegardés sont toujours verrouillés, peu importe si l'option **Verrouiller les fichiers pendant la sauvegarde** (`-lock`) est activée ou désactivée. Avec l'option `-lock` activée, tout fichier ouvert en écriture n'est pas sauvegardé. Avec l'option `-lock` désactivée, tout fichier ouvert est sauvegardé également.
- Le périphérique et le répertoire par défaut pour les procédures de commande pré et post-exécution est `/omni$root/bin`. Pour placer la procédure de commande ailleurs, la spécification de fichier doit contenir le périphérique et le chemin du répertoire au format UNIX. Par exemple :

  `/SYS$MANAGER/DP_SAVE1.COM`
- Lors de la définition des caractères de la carte de remplacement pour les filtres **Passer** (`-skip`) ou **Uniquement** (`-only`), utilisez '*' pour les caractères multiples et '?' pour les caractères simples.
- Data Protector La bibliothèque de fichiers n'est pas prise en charge sur les disques OpenVMS ODS-2.
- Sur les systèmes OpenVMS, Data Protector ne prend pas en charge les quotas de disque sur les volumes et les jeux de volumes.

  Pour effectuer une sauvegarde de données situées sur un volume pour lequel le quota de disque est activé, configurez le script de pré-exécution afin qu'il désactive le quota de disque sur le volume concerné avant le démarrage de la sauvegarde, puis configurez le script de post-exécution de sorte qu'il active le quota de disque une fois la sauvegarde terminée.

Eléments sauvegardés

La structure des répertoires et les fichiers sont sauvegardés avec les informations du système de fichiers suivantes :

- Attributs des fichiers et des répertoires
- ACL (listes de contrôle d'accès)

Les fichiers peuvent uniquement être sauvegardés à partir de volumes FILES-11 ODS-2 ou ODS-5 montés.

À propos de la sauvegarde Novell Open Enterprise Server (OES)

La procédure de sauvegarde de Novell OES est identique à la procédure de sauvegarde standard, mais présente certains aspects propres à Novell OES.

Conditions préalables

- L'Agent de disque Data Protector doit être installé sur le système Novell OES.
- L'Agent de service cible pour le système de fichiers (TSAFS) doit être chargé en mode double.

- Pour la sauvegarde NDS/eDirectory, l'Agent de service cible pour Novell Directory Services (tsands) doit être chargé.
- Pour la sauvegarde GroupWise, l'Agent de service cible pour les systèmes de fichiers (tsafsgw) doit être chargé.
- Le compte utilisateur utilisé pour la connexion aux services de sauvegarde Novell OES doit être sélectionné et enregistré dans le fichier `HPLOGIN.NLM`. N'importe quel compte utilisateur peut être utilisé, mais les fichiers et répertoires à sauvegarder seront limités à ceux du compte.
- Les services de gestion de stockage (SMS) doivent être installés sur le système Novell OES.

Limites

- La compression logicielle des données n'est pas prise en charge. Même lorsque l'option de sauvegarde Compression logicielle est sélectionnée, ceci n'a aucune influence sur les données sauvegardées.

Sauvegarde et restauration des fichiers compressés

Novell OES assure la compression des fichiers. Par défaut, Data Protector sauvegarde et donc restaure ces fichiers dans leur format compressé. De tels fichiers ne peuvent être restaurés que vers Novell OES avec des volumes compressés.

Eléments sauvegardés

- Volumes Linux natifs
- Données Novell GroupWise

Après la sauvegarde de chaque fichier, l'indicateur d'archive est effacé et la date/heure d'archivage indiquée.

Configuration de Novell OES

Enregistrement du nom d'utilisateur et du mot de passe à l'aide de l'utilitaire HPLOGIN

L'utilitaire HPLOGIN se trouve dans le répertoire `/opt/omni/lbin`. Exécutez-le pour enregistrer les informations d'identification utilisateur adéquates (nom d'utilisateur et mot de passe) dans le fichier `/root/OMNI$CFG.DAT`.

Procédure

1. Changez le répertoire de travail en cours pour `/opt/omni/lbin`.
2. Exécutez l'utilitaire HPLOGIN :

   ```
   ./hplogin
   ```

Chargement de l'agent de service cible pour les systèmes de fichiers (tsafs) en mode double

Procédure

1. Configurez le TSA sur le système cible. Par défaut, le TSA est chargé en mode Linux. Faites-le passer en mode double :
   a. Changez le répertoire de travail en cours pour `/opt/novell/sms/bin`.
   b. Vérifiez si le tsafs est déjà chargé :
      ```
      ./smsconfig -t
      ```
   c. S'il l'est, déchargez-le :
      ```
      ./smsconfig -u tsafs
      ```
   d. Chargez le TSA en mode double :
      ```
      ./smsconfig -l tsafs --tsaMode=Dual
      ```
2. Le chemin d'accès complet au fichier de configuration tsafs sous Open Enterprise Server Linux est `/etc/opt/novell/sms/tsafs.conf`. Dès que le TSA est chargé, il lit le fichier de configuration pour obtenir sa configuration par défaut. Configurez ce fichier pour charger automatiquement le TSAFS en mode double à chaque chargement du TSA.
3. Modifiez le fichier `/etc/opt/novell/sms/tsafs.conf,`, en remplaçant l'option tsamode Linux par dual et enregistrez le fichier :
   ```
   tsamode=Dual
   ```

Chargement de l'agent de service cible pour Novell Directory Services (tsands)

Vous pouvez charger l'agent tsands manuellement ou configurer son chargement automatique lors du démarrage de Novell OES.

Procédure

- Pour charger l'agent manuellement :
  1. Ouvrez une fenêtre de terminal.
  2. Changez le répertoire en cours pour `/opt/novell/sms/bin`.
  3. Exécutez la commande suivante pour vérifier si l'agent est déjà chargé :
     ```
     ./smsconfig -t
     ```
  4. Si l'agent n'est pas chargé, chargez-le :
     ```
     ./smsconfig -l tsands
     ```
- Pour configurer automatiquement le chargement de l'agent :
  1. Ajoutez la ligne suivante au fichier `/etc/opt/novell/sms/smdrd.conf` :
     ```
     autoload: tsands
     ```

Chargement de l'agent de service GroupWise pour les systèmes de fichiers (tsafsgw)

Vous pouvez charger l'agent tsafsgw manuellement ou configurer son chargement automatique lors du démarrage de Novell OES.

Procédure

- Pour charger l'agent manuellement :
  1. Ouvrez une fenêtre de terminal.
  2. Changez le répertoire en cours pour `/opt/novell/sms/bin`.
  3. Exécutez la commande suivante pour vérifier si l'agent est déjà chargé :

     `./smsconfig -t`
  4. Si l'agent n'est pas chargé, chargez-le en fournissant les paramètres appropriés :

     `./smsconfig -l tsafsgw --home` *`DomainDirectory`* `--home` *`PostOfficeDirectory`*
- Pour configurer automatiquement le chargement de l'agent :
  1. Ajoutez la ligne suivante au fichier de configuration `/etc/opt/novell/sms/smdrd.conf` (remplacez les arguments génériques par des valeurs réelles) :

     `autoload: tsafsgw --home` *`DomainDirectory`* `--home` *`PostOfficeDirectory`*

À propos des performances de sauvegarde

Lorsque vous configurez des sauvegardes, vous devez prendre en compte les différents facteurs de performance. En raison du nombre élevé de variables et de permutations, il nous est impossible de fournir des recommandations répondant aux exigences de l'ensemble des utilisateurs en fonction des niveaux d'investissement possibles. Toutefois, si vous essayez d'améliorer les performances d'une sauvegarde ou d'une restauration, il est important de prendre en compte ce qui suit :

Infrastructure

L'infrastructure a un impact considérable sur les performances des sauvegardes et des restaurations. Les facteurs les plus importants sont le parallélisme des chemins d'accès aux données et la vitesse de l'équipement.

- Sauvegardes et restaurations : en réseau ou locales ?

  L'envoi de données sur le réseau introduit un paramètre supplémentaire, le réseau ayant un effet sur les performances. Data Protector traite différemment le flux de données selon la situation :
  - Flux de données sur un réseau : disque vers mémoire vers réseau vers mémoire vers périphérique
  - Flux de données en local : disque vers mémoire vers périphérique

  Pour obtenir des performances maximales, il est recommandé d'utiliser des configurations de sauvegarde locales en cas de flux de données importants.
- Les périphériques utilisés, les ordinateurs eux-mêmes, ainsi que l'utilisation en parallèle du matériel

peuvent avoir un impact considérable sur les performances.

Vous pouvez optimiser les performances en matière de sauvegarde ou de restauration de la manière suivante :

- Définissez une simultanéité appropriée pour obtenir un fonctionnement continu des périphériques
- Optimisez la taille de segment et la taille de bloc
- Réglez le nombre de mémoires tampon d'Agent de disque
- Utilisez la compression logicielle ou la compression matérielle
- Utilisez des bibliothèques de fichiers de périphériques de sauvegarde sur disque
- Planifiez des sauvegardes complètes et incrémentales
- Utilisez des stratégies de sauvegarde avancées, telles que la sauvegarde synthétique et la sauvegarde de disque en plusieurs étapes
- Optimisez la distribution des objets sauvegarde sur les supports
- en désactivant l'analyse de système de fichiers.

Mise en miroir d'objets et performances de sauvegarde

La mise en miroir d'objet a une incidence sur les performances de sauvegarde. Sur les clients Gestionnaire de cellule et Agent de support, l'impact de l'écriture de miroirs est le même que celui de la sauvegarde d'objets supplémentaires. Sur ces systèmes, les performances diminuent en fonction du nombre de miroirs. Sur les clients Agents de disque, la mise en miroir ne provoque aucun impact, car les objets sauvegarde ne sont lus qu'une fois.

Les performances dépendent également de facteurs tels que la taille des blocs des périphériques et le type de connexion des périphériques. Si les périphériques utilisés pour la sauvegarde et la mise en miroir d'objets ont des tailles de bloc différentes, les données enregistrées dans les miroirs sont réassemblées durant l'opération, ce qui demande davantage de temps et de ressources. Si les données doivent être transférées par l'intermédiaire d'un réseau, il faut en outre tenir compte de la charge du réseau et de la durée du transfert.

Matériel hautes performances autre que les périphériques

Les opérations de lecture du disque et d'écriture sur le périphérique peuvent être directement influencées par la vitesse des ordinateurs eux-mêmes. Les systèmes sont chargés lors d'une sauvegarde par la lecture du disque, par la (dé)compression logicielle, etc.

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

Parallélisme de matériel

L'utilisation en parallèle de plusieurs chemins de données constitue un excellent moyen pour optimiser les performances. Cela comprend l'infrastructure réseau. Le parallélisme est utile dans les cas suivants :

- Lorsque plusieurs systèmes sont sauvegardés en local, c'est-à-dire lorsque le ou les disques et les périphériques correspondants sont connectés au même système.
- Lorsque plusieurs systèmes sont sauvegardés via le réseau. Dans ce cas, le routage du trafic sur le réseau doit être tel que les chemins de données ne se chevauchent pas, sinon cela entraîne une baisse de performance.
- Lorsque plusieurs objets (disques) sont sauvegardés vers un ou plusieurs périphériques (à bandes).
- Lorsque plusieurs liens réseau dédiés entre certains systèmes peuvent être utilisés. Par exemple, 6 objets (disques) à sauvegarder se trouvent sur le système A, et le système B est doté de 3 périphériques à bandes rapides. La solution est de dédier 3 liens réseau à la sauvegarde entre le système A et le système B.
- Si plusieurs périphériques sont utilisés et que l'option **Partage de charge** est activée.

Simultanéité

Le nombre d'Agents de disque lancés pour chaque Agent de support est appelé simultanéité (de sauvegarde) des Agents de disque ; il est modifiable grâce aux options avancées relatives au périphérique ou au moment de la configuration d'une sauvegarde. La simultanéité définie dans la spécification de sauvegarde prévaut sur celle définie dans la définition du périphérique.

Data Protector fournit par défaut un nombre d'Agents de disque suffisant pour la plupart des situations. Par exemple, pour un périphérique DDS standard, deux Agents de disque envoient suffisamment de données pour que le périphérique fonctionne en mode continu. Si vous utilisez un périphérique de bibliothèque équipé de plusieurs lecteurs et que chaque lecteur est contrôlé par un Agent de support, vous pouvez régler la simultanéité indépendamment pour chaque lecteur.

Impact sur les performances

Si la simultanéité de la sauvegarde est correctement définie, les performances en sont considérablement augmentées. Par exemple, si un périphérique de bibliothèque dispose de quatre lecteurs, chacun étant contrôlé par un Agent de support et chaque Agent de support recevant des données de deux Agents de disque simultanément, les données de huit disques sont sauvegardées simultanément.

Flux à données multiples

Vous pouvez sauvegarder les parties d'un disque de façon simultanée sur plusieurs périphériques. Cette méthode accélère la sauvegarde. Elle est très pratique pour la sauvegarde de disques rapides et volumineux sur des périphériques relativement lents. Plusieurs Agents de disque lisent les données du disque en parallèle et les envoient à plusieurs Agents de support.

Si un point de montage a été sauvegardé via plusieurs Agents de disque, les données se trouvent sur plusieurs objets. Pour restaurer la totalité du point de montage, vous devez définir toutes les parties de celui-ci dans une spécification de sauvegarde unique, puis restaurer l'ensemble de la session.

Périphériques en mode continu

Pour optimiser la performance d'un périphérique, celui-ci doit fonctionner en continu. Un périphérique fonctionne en mode continu s'il peut fournir un volume de données suffisant au support pour que celui-ci avance en continu. Si ce n'est pas le cas, l'avancement de la bande est interrompu, le périphérique attend d'avoir reçu d'autres données, fait légèrement reculer la bande, puis reprend l'écriture des données, et ainsi de suite. En d'autres termes, si le taux de données écrit sur la bande est inférieur ou égal à celui que le périphérique peut recevoir du système informatique, le périphérique fonctionne en mode continu. Le fonctionnement en mode continu d'un périphérique dépend également d'autres facteurs, tels que la charge du réseau et la taille de bloc des données écrites sur le périphérique de sauvegarde en une opération. Dans des infrastructures de sauvegarde en réseau, ces aspects doivent retenir votre attention. Pour les sauvegardes locales, où les disques et les périphériques sont reliés au même système, une simultanéité de 1 peut suffire si vos disques sont suffisamment rapides.

Procédure à suivre pour la configuration d'un périphérique en mode continu

Pour permettre au périphérique de fonctionner en mode continu, il faut lui envoyer une quantité de données suffisante. Pour cela, Data Protector démarre plusieurs Agents de disque pour chaque Agent de support écrivant des données sur le périphérique.

Taille de bloc

Les segments ne sont pas écrits sous forme d'une unité entière, mais plutôt en sous-unités de taille inférieure appelées blocs. Le périphérique traite les données qu'il reçoit avec une taille de bloc spécifique au type de périphérique.

Data Protector utilise une taille de bloc de périphérique par défaut concernant différents types de périphérique. La taille de bloc s'applique à tous les périphériques créés par Data Protector et à l'Agent de support exécutés sur les différentes plates-formes.

Vous pouvez améliorer les performances en augmentant la taille de bloc. Vous pouvez régler la taille des blocs envoyés au périphérique lors de la configuration d'un périphérique ou de la modification de ses propriétés avec les options Avancé du périphérique. Une restauration utilise la taille de bloc.

ATTENTION :
Avant d'augmenter la taille de bloc d'un périphérique contrôlé par l'Agent de support Data Protector exécuté sur un système d'exploitation donné, vérifiez que la taille de bloc désirée ne dépasse pas la taille de bloc maximale par défaut prise en charge par le système d'exploitation. Si la limite est dépassée, Data Protector ne peut pas restaurer les données à partir d'un tel périphérique. Pour plus d'informations sur les conditions et la façon d'ajuster la taille de bloc maximale prise en charge, consultez la documentation du système d'exploitation.

Vous devez modifier la taille de bloc avant de formater des bandes. La taille de bloc du périphérique est écrite dans l'en-tête d'un support, de sorte que Data Protector connaisse la taille à utiliser. Si la taille de bloc du périphérique diffère de la taille de bloc du support, une erreur survient.

Toutefois, avant de changer la taille de bloc du périphérique, vous devez vérifier la taille de bloc supportée par la carte hôte utilisée. La taille de bloc minimale des anciennes cartes SCSI, comme Adaptec 2940, était de 56 Ko. La taille de bloc minimale utilisée principalement avec les nouvelles cartes SCSI est de 64 Ko.

Vous pouvez augmenter la taille de bloc maximale sur un client Agent de support Windows en modifiant son registre. La procédure dépend du type de carte bus hôte : SCSI, Fibre Channel ou iSCSI. Pour plus d'informations, consultez l'exemple de rubrique connexe.

Avant de modifier la taille de bloc d'une carte bus hôte donnée, reportez-vous à la documentation du fournisseur ou contactez le service d'assistance de ce fournisseur.

Taille de segment

Un support est constitué de segments de données, de catalogue et d'un en-tête. Les informations d'en-tête sont stockées dans le segment d'en-tête, dont la taille est identique à la taille du bloc. Les données sont enregistrées dans des blocs de données des segments de données. Les informations concernant chaque segment de données sont stockées dans le segment de catalogue correspondant. Ces informations sont tout d'abord stockées dans la mémoire de l'Agent de support, puis écrites dans un segment de catalogue sur le support, ainsi que dans la base de données IDB.

La taille du segment, mesurée en méga-octets, représente la taille maximale des segments de données. Si vous sauvegardez un grand nombre de petits fichiers, la taille de segment réelle peut être limitée par la taille maximale des segments de catalogue. Configurable par l'utilisateur pour chaque périphérique, cette taille a un impact sur les performances au cours des opérations de restauration et d'importation de supports. Vous pouvez régler la taille de segment lors de la configuration d'un périphérique ou de la modification de ses propriétés avec les options Avancé du périphérique.

La taille de segment optimale dépend du type de support utilisé dans le périphérique et du type des données à sauvegarder. Le nombre moyen de segments par bande est de 50. La taille de segment par défaut peut être calculée en divisant la capacité d'origine d'une bande par 50. La taille de catalogue maximale est limitée à une valeur fixe (12 Mo) pour tous les types de supports.

Data Protector termine un segment lorsque la première limite est atteinte. Si vous sauvegardez un grand nombre de petits fichiers, la limite de catalogue des supports est atteinte plus vite, ce qui peut donner des tailles de segment réduites.

Nombre de mémoires tampon d'Agent de disque

Les Agents de support et les Agents de disque Data Protector utilisent des mémoires tampons pour stocker les données à transférer. La mémoire est divisée en plusieurs zones tampon (une pour chaque Agent de disque, en fonction du nombre de périphériques fonctionnant simultanément). Chaque zone tampon est composée de 8 Mémoires tampon d'Agent de disque (de la même taille que celle du bloc configuré pour le périphérique).

Bien que cela soit rarement nécessaire, vous pouvez modifier cette valeur lorsque vous configurez un nouveau périphérique ou lorsque vous modifiez les propriétés d'un périphérique en utilisant ses options avancées. Ces paramètres peuvent être changés pour deux raisons principales :

- Mémoire insuffisante : la mémoire partagée requise pour un Agent de support peut être calculée comme suit :

  ```
  DAConcurrency*NumberOfBuffers*BlockSize
  ```

  Si vous réduisez le nombre de mémoires tampon de 8 à 4, par exemple, la consommation de mémoire sera réduite de 50 % ; cette opération modifiera également les performances.
- Mode continu

  Si la bande passante du réseau disponible varie de façon significative au cours de la sauvegarde, l'Agent de support doit avoir suffisamment de données prêtes à être écrites afin que le périphérique fonctionne en mode continu. Dans ce cas, vous devez augmenter le nombre de mémoires tampon.

Compression logicielle

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

La compression logicielle est désactivée par défaut. Généralement, seule la compression matérielle doit être utilisée pour améliorer la performance. La compression logicielle ne doit être utilisée que pour la sauvegarde de plusieurs systèmes sur un réseau lent permettant la compression des données avant leur envoi.

Pensez à désactiver la compression matérielle lorsque vous utilisez la compression logicielle, car deux opérations de compression ont pour effet d'augmenter le volume des données.

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.

La compression matérielle est effectuée par un périphérique qui reçoit les données originales de l'Agent de support et les écrit sur la bande sous forme compressée. Ce procédé permet d'augmenter la vitesse à laquelle un lecteur de bande reçoit les données car le volume de données écrit sur la bande est moins important.

Gardez à l'esprit les remarques suivantes concernant la compression matérielle :

- La compression matérielle doit être utilisée avec précaution, car les supports sur lesquels figurent des données compressées ne peuvent pas être lus avec un périphérique en mode non compressé et vice versa.
- N'utilisez pas la compression logicielle et la compression matérielle en même temps, car la double compression entraîne une baisse de performance sans pour autant améliorer la compression.
- Les lecteurs Ultrium LTO HPE utilisent la compression matérielle automatique, qui ne peut pas être désactivée. Il est donc recommandé de laisser la compression logicielle désactivée lorsque vous configurez un lecteur HPE Ultrium LTO avec Data Protector.
- En cas de lecture sur un support écrit avec compression matérielle à l'aide d'un périphérique ne la prenant pas en charge, Data Protector ne parvient pas à identifier le support et à lire les données. Un tel support est traité comme inconnu ou nouveau.

Lorsque vous configurez le périphérique, si vous sélectionnez l'adresse SCSI dans la liste déroulante, Data Protector détermine automatiquement si le périphérique peut utiliser la compression matérielle.

Sur les systèmes UNIX, vous pouvez activer la compression matérielle en sélectionnant un fichier de périphérique de compression matérielle.

Sur les systèmes Windows, si la détection échoue et si vous entrez manuellement l'adresse SCSI, ajoutez `C` à la fin de l'adresse SCSI du périphérique/du lecteur, par exemple : `scsi:0:3:0C` (ou `tape2:0:1:0C` si le lecteur de bandes est chargé). Si le périphérique prend en charge la compression matérielle, celle-ci sera utilisée ; sinon, l'option `C` sera ignorée.

Pour désactiver la compression matérielle sous Windows, ajoutez `N` à la fin des adresses SCSI de périphérique/lecteur, par exemple : `scsi:0:3:0N`.

Dans le cas de périphériques à chemins multiples, cette option est définie séparément pour chaque chemin.

Sauvegarde d'image disque ou sauvegarde de système de fichiers

Lorsque vous choisissez entre une sauvegarde d'image disque et une sauvegarde de système de fichiers, vous devez tenir compte des avantages et des inconvénients. Dans la plupart des cas, la sauvegarde de système de fichiers est recommandée.

	Sauvegarde de système de fichiers	**Sauvegarde d'image disque**
Cohérence de sauvegarde	Les fichiers peuvent être verrouillés pendant la sauvegarde et sont sauvegardés dans un état cohérent. La structure des fichiers et des répertoires est préservée.	Les fichiers ne sont pas verrouillés pendant la sauvegarde et sont sauvegardés dans un état à un instant donné. La structure des fichiers et des répertoires ne peut pas être explorée.
Taille de sauvegarde	L'espace occupé par les données sauvegardées est le même que la taille cumulée des données des fichiers et dossiers au moment de la sauvegarde.	L'espace occupé par les données sauvegardées sur les supports de sauvegarde est le même que la taille du volume sauvegardé original.
Vitesse de sauvegarde et de restauration	La vitesse de sauvegarde et de restauration est plus élevée si un disque sauvegardé n'est pas plein et que le nombre de fichiers est faible.	La vitesse de sauvegarde et de restauration est plus élevée si un disque sauvegardé est plein et que le nombre de petits fichiers est élevé.
Possibilités d'utilisation de la restauration	Il est plus facile de parcourir les fichiers restaurés car la structure des fichiers et des répertoires est préservée.	Le disque entier ou une partie du disque sont restaurés, la structure des fichiers et des répertoires ne peut pas être explorée.

REMARQUE :
Sur les systèmes Windows, vous pouvez activer une sauvegarde d'image disque en utilisant des modules d'écriture VSS. Ainsi, le volume n'est pas verrouillé pendant la sauvegarde et d'autres applications peuvent y accéder. C'est important lorsque vous sauvegardez un volume

Système.

Distribution des objets sur les supports

Vous pouvez configurer une sauvegarde de telle manière que les données sauvegardées soient copiées sur les supports dans plusieurs configurations différentes. Par exemple, vous pouvez configurer une sauvegarde dans laquelle un objet est sauvegardé sur un support ou plusieurs objets sur plusieurs supports, chaque support contenant des données de chaque objet.

Dans certaines conditions, une distribution donnée augmentera les performances de la sauvegarde, mais ne sera pas optimale au niveau de la configuration de la restauration. Vous devez donc définir votre stratégie de sauvegarde afin d'optimiser la configuration d'une sauvegarde (car cette opération est effectuée fréquemment) et en même temps de permettre une restauration d'un niveau acceptable.

Analyse de systèmes de fichiers

Avant de sauvegarder les fichiers, Data Protector effectue une analyse de l'arborescence sélectionnée pour la sauvegarde. Cette procédure peut avoir une incidence sur les performances. L'impact étant négligeable avec l'analyse rapide de systèmes de fichiers sur des systèmes Windows et la fonction d'analyse de systèmes de fichiers sur des systèmes UNIX, il n'est pas recommandé de modifier les paramètres par défaut uniquement dans un but de performance.

L'analyse des systèmes de fichiers peut varier selon le système à sauvegarder :

Système	Fonction d'analyse de systèmes de fichiers	Pour désactiver la fonction
Windows	Analyse rapide de systèmes de fichiers (toujours sélectionnée)	Vous pouvez désactiver le système de fichiers en réglant l'option `OB2NOTREEWALK` `omnirc` sur `1`.
	Détecter liens réels NTFS (par défaut : non sélectionné)	La sélection de l'option Détecter liens réels NTFS entraîne une réduction significative de la performance. N'activez cette option qu'en cas de présence de liens réels NTFS.
UNIX	Détecter les liens réels et calculer la taille (par défaut : sélectionné)	La sélection de l'option **Sauvegarder les liens réels POSIX en tant que fichiers** désactive l'analyse du système de fichiers.

Diverses astuces pour améliorer les performances

Vous pouvez optimiser les performances de sauvegarde ou de restauration en utilisant les astuces ci-dessous.

Amélioration des	Comment améliorer les performances ?

performances	
Correctifs	Vérifiez que vous avez installé tous les correctifs se rapportant aux performances sur le réseau.
Emplacement des périphériques	Utilisez des périphériques locaux partout où cela s'avère possible.
Cartes réseau	Vous pouvez remonter une carte FDDI sur le bus afin qu'elle ait une priorité plus haute. Utilisez le protocole FTP pour transférer les fichiers volumineux entre le système Agent de support et le système Agent de disque pour comparer le taux de transfert aux performances Data Protector. Attention : les cartes réseau configurées en semi-duplex entraînent une baisse de performance.
Périphérique à grande vitesse	Vous pouvez simuler un périphérique à grande vitesse sur le client Agent de support si vous pensez que le taux de transfert des données vers le périphérique à bandes est trop faible, ou que le périphérique ne peut pas traiter correctement le flux de données.
Configuration des périphériques	Vous pouvez régler la taille des blocs envoyés au périphérique afin d'améliorer les performances.
Contrôle CRC	Vous pouvez désactiver l'option Contrôle CRC. Lorsqu'elle est activée, cette option a une incidence sur les performances en raison du calcul de CRC effectué par le client Agent de support.
Journalisation et niveau de rapport	Vous pouvez désactiver la journalisation en la mettant sur Pas de journalisation si une mise à jour de la Base de données interne (IDB) prend trop de temps. Vous pouvez filtrer les messages en mettant le Niveau de rapport sur Critique.
Clients d'application Data Protector	Vous pouvez diminuer la valeur `SmWaitforNewClient` si une session de restauration des clients d'application (Oracle, SAP R/3) prend trop de temps. Définissez-la sur une valeur inférieure à la valeur par défaut (5 minutes).

Chapitre 11: Consolidation d'objet

À propos de la consolidation d'objet

L'option de consolidation d'objets de Data Protector vous permet de fusionner une chaîne de restauration d'un objet de sauvegarde dans une nouvelle version consolidée de cet objet. Grâce à cette option, vous n'avez plus besoin d'exécuter des sauvegardes complètes. Au lieu de cela, vous pouvez exécuter indéfiniment des sauvegardes incrémentales et consolider la chaîne de restauration selon vos besoins.

Pendant la session de consolidation d'objets, Data Protector lit les données sauvegardées à partir du support source, les fusionne et écrit la version consolidée sur le support cible. Le résultat d'une session de consolidation d'objets est une sauvegarde complète synthétique de la version d'objet que vous avez spécifiée.

Types de consolidation d'objets

Vous pouvez démarrer une session de consolidation d'objets de façon interactive ou définir un démarrage automatique de la session. Data Protector propose deux types de consolidation d'objets automatisée : la consolidation d'objets post-sauvegarde et la consolidation d'objets planifiée.

Consolidation d'objets post-sauvegarde

La consolidation d'objets post-sauvegarde a lieu après une session de sauvegarde qui est spécifiée dans la spécification de consolidation d'objets automatisée. Elle consolide les objets sélectionnés en fonction de la spécification de consolidation d'objets automatisée, qui ont été écrits au cours de la session concernée.

Consolidation d'objets planifiée

La consolidation d'objets planifiée a lieu à l'heure définie par l'utilisateur. Les objets sauvegardés pendant différentes sessions de sauvegarde peuvent être consolidés au cours d'une même session de consolidation d'objets planifiée.

Comment consolider des objets

Commencez par créer une spécification de consolidation d'objet. Dans la spécification, sélectionnez l'objet à consolider, les supports et les périphériques à utiliser et les options de session.

Sélection des périphériques

Vous devez utiliser différents périphériques pour lire les sauvegardes complètes, lire les sauvegardes incrémentales et écrire la sauvegarde complète synthétique. Les périphériques cibles peuvent avoir une taille de bloc supérieure aux périphériques sources. Néanmoins, pour éviter de dégrader les performances, il est préférable que les périphériques aient la même taille de bloc et soient connectés au même système.

Les périphériques qui ne sont pas disponibles au début d'une session ne peuvent pas être utilisés pendant celle-ci. En cas d'erreur de support, le périphérique concerné sera évité pendant la session.

Options de consolidation d'objet

Vous pouvez activer le filtrage d'objets sources et spécifier la protection de données, la protection de catalogue et le niveau de journalisation dans la spécification de consolidation d'objet. Des équivalents de la plupart de ces options sont également utilisés pour la sauvegarde.

Sélection du jeu de supports

Si une version d'objet à consolider a donné lieu à des copies résidant sur différents jeux de supports, vous pouvez employer n'importe quel jeu de supports comme source. Par défaut, Data Protector sélectionne automatiquement le jeu de supports le plus approprié. Vous pouvez influer sur cette sélection en spécifiant la priorité d'emplacement des supports.

Le processus global de sélection des supports est le même que pour la restauration. En cas de consolidation d'objets interactive, vous pouvez sélectionner manuellement le jeu de supports à utiliser. Lors de la configuration d'une consolidation automatisée, vous ne pouvez pas sélectionner de supports car la sauvegarde des objets est souvent effectuée plus tard.

Propriété des objets consolidés

Le propriétaire des objets consolidés est le propriétaire des objets de sauvegarde original, non l'utilisateur Data Protector invoquant la session de consolidation d'objet.

Tâches de consolidation d'objet standard

Voici les conditions préalables et les limites de la fonction de consolidation d'objet :

Conditions préalables

- Toutes les sauvegardes qui seront consolidées ont été effectuées avec l'option Sauvegarde incrémentale avancée activée.
- Toutes les sauvegardes incrémentales qui seront consolidées résident dans une bibliothèque de fichiers ou un périphérique B2D (sauf Smart Cache).
- La chaîne de restauration est complète, ce qui signifie que toutes les versions d'objet qui la composent ont le statut `Completed` ou `Completed/Errors` et que tous les supports contenant ces versions d'objet sont disponibles.
- Les périphériques de sauvegarde nécessaires doivent être configurés et les supports préparés.
- Vous devez installer un Agent de support sur chaque système qui participera à la session de consolidation d'objet.
- Vous devez disposer des droits utilisateur appropriés pour démarrer une session de consolidation d'objet. Les mêmes droits utilisateur s'appliquent comme pour la sauvegarde.

- Pour effectuer une sauvegarde complète virtuelle, toutes les sauvegardes (complète, incrémentale et virtuelle complète) doivent résider dans une bibliothèque de fichiers utilisant un format de support de fichiers distribué.

Limites

- Les périphériques cibles doivent avoir une taille de bloc égale ou supérieure à celle des périphériques sources.
- Un même support ne peut pas être utilisé comme support source et support cible dans la même session de consolidation d'objet.
- Les supports sources en cours de lecture ne sont pas disponibles pour la restauration.
- La consolidation d'objet n'est pas disponible pour les objets sauvegardés à l'aide du cryptage AES 256 bits.

  la consolidation d'objet est prise en charge pour tous les périphériques B2D, sauf Smart Cache.

> **REMARQUE :**
> Lorsque vous modifiez le paramètre Compression logicielle ou Encoder de la spécification de sauvegarde, une sauvegarde complète doit être effectuée comme base d'une consolidation d'objet ultérieure.

Consolidation d'objet interactive

Vous pouvez sélectionner des objets en vue d'une consolidation interactive à partir du point de départ Supports, Objets ou Sessions, selon vos besoins Vous ne pouvez pas enregistrer une spécification de consolidation d'objets interactive ; vous pouvez uniquement lancer une session de consolidation d'objets.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez l'élément **Consolidation**, puis l'élément **Interactive**.
3. Cliquez sur **Objets** ou **Sessions** pour ouvrir l'assistant.
   - Si vous choisissez **Objets**, la liste des objets apparaît.
   - Si vous choisissez **Sessions**, la liste des sessions au cours desquelles des objets ont été écrits sur des supports apparaît.
4. Sélectionnez des instants pour les objets à consolider. Vous ne pouvez pas sélectionner de sauvegardes complètes car, en tant que telles, elles ne peuvent pas être consolidées.

   Le choix d'un point dans le temps sélectionne la chaîne de restauration complète. S'il existe plusieurs chaînes de restauration pour la même version, elles sont toutes sélectionnées, mais une seule va en fait être utilisée. Votre sélection est signalée en bleu, les autres sauvegardes incrémentales incluses dans la chaîne de restauration en noir et la sauvegarde complète correspondante en gris (grisé). La coche bleue indique la version qui sera consolidée.

Vous pouvez sélectionner plusieurs instants donnés pour la consolidation et les chaînes de restauration peuvent se chevaucher. Si vous sélectionnez un instant possédant déjà une coche noire, la coche devient bleue.

Pour désélectionner une chaîne de restauration, cliquez sur la coche bleue. La chaîne de restauration complète est désélectionnée, à moins que certaines versions d'objet n'appartiennent à une autre chaîne, auquel cas elles restent sélectionnées avec une coche noire.

Cliquez sur **Suivant**.

5. Spécifiez les périphériques qui vont lire les sauvegardes incrémentales et les complètes.

   Limitez la consolidation d'objets à des bibliothèques de fichiers ou des périphériques B2D spécifiques (sauf Smart Cache) en les sélectionnant en tant que périphériques de lecture pour les sauvegardes incrémentales. Seuls les objets résidant dans les périphériques spécifiés seront consolidés.

   Par défaut, les périphériques de lecture pour les sauvegardes complètes sont ceux utilisés pour la sauvegarde dans les spécifications de sauvegarde sélectionnées. Vous pouvez les modifier, le cas échéant. Cliquez sur **Suivant**.
6. Sélectionnez les périphériques cibles pour l'opération de consolidation d'objets. Data Protector sélectionne les périphériques les plus adaptés à partir de ceux que vous indiquez ici. Cliquez sur **Suivant**.
7. Spécifiez des options si nécessaire. Cliquez sur **Suivant**.
8. La liste des supports contenant les objets sélectionnés s'affiche.

   Lorsqu'un même objet réside sur plusieurs jeux de supports, vous pouvez modifier la priorité d'emplacement des supports pour influer sur leur sélection.

   Cliquez sur **Suivant**.
9. Contrôlez les versions d'objet impliquées dans l'opération. S'il existe d'autres chaînes de restauration, il se peut que toutes les versions d'objet répertoriées ne soient pas utilisées. Cliquez sur **Suivant**.
10. Consultez le récapitulatif des instants sélectionnés. Pour modifier des options pour un instant donné, sélectionnez-le dans la liste et cliquez sur **Propriétés**.
11. Cliquez sur **Terminer** pour quitter l'assistant.

Configuration de la consolidation d'objet post-sauvegarde

La consolidation d'objets post-sauvegarde a lieu après une session de sauvegarde qui est spécifiée par le nom de la spécification de sauvegarde dans la spécification de consolidation d'objets automatisée. Elle consolide les objets sauvegardés au cours de la session de sauvegarde qui correspondent aux critères spécifiés.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez **Consolidation**, puis **Automatisé**.

3. Cliquez sur **Post-sauvegarde** avec le bouton droit de la souris, puis cliquez sur **Ajouter** pour ouvrir l'assistant.
4. Sélectionnez les spécifications de sauvegarde qui contiennent les objets à consolider. Cliquez sur **Suivant**.
5. Spécifiez le filtre d'objet pour l'opération de consolidation. Cliquez sur **Suivant**.
6. Spécifiez les périphériques qui vont lire les sauvegardes incrémentales et les complètes.

   Limitez la consolidation d'objets à des bibliothèques de fichiers ou des périphériques B2D spécifiques (sauf Smart Cache) en les sélectionnant en tant que périphériques de lecture pour les sauvegardes incrémentales. Seuls les objets résidant dans les périphériques spécifiés seront consolidés.

   Par défaut, les périphériques de lecture pour les sauvegardes complètes sont ceux utilisés pour la sauvegarde dans les spécifications de sauvegarde sélectionnées. Vous pouvez les modifier, le cas échéant. Cliquez sur **Suivant**.
7. Sélectionnez les périphériques cibles pour l'opération de consolidation d'objets. Data Protector sélectionne les périphériques les plus adaptés à partir de ceux que vous indiquez ici. Cliquez sur **Suivant**.
8. Spécifiez des options si nécessaire. Cliquez sur **Suivant**.
9. Cliquez sur **Enregistrer sous...**, entrez un nom de spécification, puis cliquez sur **OK** pour enregistrer la spécification de consolidation d'objets post-sauvegarde.

Planification d'une consolidation d'objets

La consolidation d'objets planifiée a lieu à l'heure définie par l'utilisateur. Elle consolide les objets qui correspondent aux critères spécifiés. Les objets sauvegardés pendant différentes sessions de sauvegarde peuvent être consolidés au cours d'une même session de consolidation d'objets planifiée.

Si plusieurs chaînes de restauration sont disponibles, Data Protector consolide celle contenant la version de l'objet avec le dernier point dans le temps. Par exemple, les sessions de sauvegarde : Complète, Incr1, Incr2, Incr2, Incr2 créent trois chaînes de restauration mais Data Protector consolide uniquement celle contenant les sauvegardes Complète, Incr1 et la dernière version Incr2.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez **Consolidation**, puis **Automatisé**.
3. Cliquez sur **Planifiée** avec le bouton droit de la souris, puis cliquez sur **Ajouter** pour ouvrir l'assistant.
4. Sélectionnez les spécifications de sauvegarde qui contiennent les objets à consolider. Cliquez sur **Suivant**.
5. Spécifiez le filtre temporel pour l'opération de consolidation d'objets. Seuls les objets qui ont été sauvegardés dans la période spécifiée seront consolidés. Cliquez sur **Suivant**.
6. Spécifiez le filtre d'objet pour l'opération de consolidation. Cliquez sur **Suivant**.
7. Spécifiez les périphériques qui vont lire les sauvegardes incrémentales et les complètes.

Limitez la consolidation d'objets à des bibliothèques de fichiers ou des périphériques B2D spécifiques (sauf Smart Cache) en les sélectionnant en tant que périphériques de lecture pour les sauvegardes incrémentales. Seuls les objets résidant dans les périphériques spécifiés seront consolidés.

Par défaut, les périphériques de lecture pour les sauvegardes complètes sont ceux utilisés pour la sauvegarde dans les spécifications de sauvegarde sélectionnées. Vous pouvez les modifier, le cas échéant. Cliquez sur **Suivant**.

8. Sélectionnez les périphériques cibles pour l'opération de consolidation d'objets. Data Protector sélectionne les périphériques les plus adaptés à partir de ceux que vous indiquez ici. Cliquez sur **Suivant**.
9. Spécifiez des options si nécessaire. Cliquez sur **Suivant**.
10. Cliquez sur **Enregistrer et planifier...** Entrez un nom de spécification, puis cliquez sur **OK** pour enregistrer la spécification de consolidation d'objet planifiée. Une fois la spécification enregistrée, l'assistant de planification s'ouvre. Suivez les étapes de l'assistant pour planifier la spécification.

    Pour plus d'informations sur la création et la modification de planifications dans Data Protector à l'aide du planificateur, consultez la rubrique *Planificateur, Page 110*.

    > **IMPORTANT :**
    > Avec Data Protector10.00, le planificateur de base et le planificateur avancé sont devenus obsolète et ont été remplacés par un nouveau planificateur basé sur Internet. Vous pouvez configurer des sauvegardes sans surveillance en planifiant des sessions de sauvegarde à exécuter à des instants précis.
    >
    > Lors de la mise à niveau vers Data Protector, toutes les planifications Data Protector existantes sont automatiquement migrées vers le nouveau planificateur.

Copie d'une spécification de consolidation d'objet

Vous pouvez copier une consolidation d'objets déjà configurée et enregistrée.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez **Consolidation**, **Automatisée**, puis **Post sauvegarde**. Toutes les spécifications de consolidation d'objets enregistrées s'affichent alors.
3. Dans la zone de résultats, cliquez avec le bouton droit de la souris sur la spécification de consolidation d'objet à copier, puis sélectionnez **Copier sous**. La boîte de dialogue Copier sous s'affiche.
4. Dans la zone de texte Nom, attribuez un nom à la spécification de consolidation d'objets copiée.
5. Cliquez sur **OK**.

La spécification de consolidation d'objets copiée s'affiche dans le contexte des opérations sur les objets de la fenêtre de navigation ainsi que dans la zone de résultats sous son nouveau nom.

Chapitre 12: Copie

À propos de la duplication des données sauvegardées

La duplication de données sauvegardées présente plusieurs avantages. Vous pouvez copier des données pour améliorer leur sécurité et leur disponibilité, ou pour des raisons opérationnelles.

Data Protector fournit les méthodes suivantes de duplication des données sauvegardées : copie d'objets, mise en miroir d'objets, copie de supports et réplication sur des périphériques Backup to Disk (B2D).

	Copie d'objets	**Réplication**	**Miroir d'objet**	**Copie de supports**
Éléments dupliqués	N'importe quelle combinaison de versions d'objets appartenant à une ou plusieurs sessions de sauvegarde, copie ou consolidation d'objets.	Un ensemble d'objets issu d'une session de sauvegarde, de copie ou de consolidation d'objets	Un ensemble d'objets issu d'une session de sauvegarde	Un support complet
Quand effectuer la duplication	A tout moment à l'issue d'une sauvegarde	A tout moment à l'issue d'une sauvegarde	Pendant la sauvegarde	A tout moment à l'issue d'une sauvegarde
Type des supports sources et cibles	Peut être différent	Les données peuvent être répliquées uniquement vers des périphériques B2D de même type	Peut être différent	Doit être identique
Taille des supports sources et cibles	Peut être différent	Le périphérique cible doit disposer de suffisamment d'espace pour les données dédupliquées	Peut être différent	Doit être identique

Possibilité d'ajout des supports cibles	Oui	Non	Oui	Non [1]
Résultat de l'opération	Supports contenant les versions d'objet sélectionnées	Une copie identique stockée sur le même périphérique B2D cible	Supports contenant les versions d'objet sélectionnées	Supports identiques aux supports sources

À propos de la copie d'objets

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

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

Le résultat d'une session de copie d'objets est un jeu de supports contenant des copies des versions d'objet spécifiées.

Voici les caractéristiques de la fonction de copie d'objets :

- Démarrage de la session

  Une session de copie d'objets peut être démarrée de manière interactive ou automatique.
- Sélection des supports

  Vous pouvez utiliser comme supports sources des jeux de supports d'origine contenant des sauvegardes, des jeux de supports contenant des copies d'objets ou des jeux de supports qui sont des copies de supports.

  Toutefois, la sélection des jeux de supports n'est pas possible après le démarrage de la session de copie d'objets. En cas de demande de montage, vous devez fournir le support qui est demandé par Data Protector ou sa copie exacte (créée à l'aide de la fonction de copie de supports).
- Type de support

  Vous pouvez copier des objets sur des supports d'un autre type. De plus, la taille de bloc du périphérique cible peut être égale ou supérieure à celle du périphérique source.
- Stratégie relative aux supports

[1] Vous pouvez utiliser comme supports cibles uniquement des supports non formatés, vides ou dont la protection a expiré. Après l'opération, les supports sources et cibles sont sans possibilité d'ajout.

Vous pouvez également combiner ces méthodes de duplication. Par exemple, vous pouvez créer des copies d'objets ou des copies de supports pour des données qui résultent d'une mise en miroir d'objets. Vous pouvez aussi copier intégralement des supports contenant des copies d'objets.

Vous pouvez ajouter des données aux supports qui contiennent déjà des sauvegardes ou des copies d'objets.

- Stratégie de protection

  Vous pouvez définir de façon indépendante les périodes de protection des objets sources et des copies d'objets.

Vous pouvez démarrer une session de copie d'objets de façon interactive ou définir un démarrage automatique de la session.

Copie d'objets automatisée

Une spécification de copie d'objets automatisée consiste à définir un ou plusieurs critères pour la sélection des versions d'objet à copier :

- Spécifications de sauvegarde - pour ne copier que des versions d'objet sauvegardées au moyen de certaines spécifications.
- Spécifications de copie d'objets - pour ne copier que les versions d'objets copiées au moyen de spécifications de copie d'objets spécifiques.
- Spécifications de consolidation d'objets - pour ne copier que les versions d'objets consolidées au moyen de spécifications de consolidation d'objets spécifiques.
- Protection des données - pour ne copier que des versions d'objets protégées.
- Nombre de copies existantes - pour ne copier que les versions d'objet ne comportant pas plus que le nombre de copies réussies indiqué.
- Bibliothèques - pour ne copier que les versions d'objet se trouvant sur les supports des bibliothèques indiquées.
- Période (uniquement en cas de spécification de copie d'objets planifiée) - pour ne copier que des versions d'objet sauvegardées dans la période indiquée.

Data Protector propose deux types de copie d'objets automatisée : la copie d'objets post-sauvegarde et la copie d'objets planifiée.

Copie d'objets post-sauvegarde

La copie d'objets post-sauvegarde, post-copie et post-consolidation (sous-ensembles de la copie d'objets post-sauvegarde), s'effectue après l'achèvement d'une session spécifiée dans la spécification de copie d'objets automatique. Elle copie les objets sélectionnés en fonction de la spécification de copie d'objets automatisée, qui ont été écrits au cours de la session concernée.

Copie d'objets planifiée

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

Comment copier des objets

Commencez par cérer une spécification de copie d'objet Dans la spécification, sélectionnez les objets à copier, les supports et les périphériques à utiliser, les options de session et la priorité des

emplacements des supports qui influe sur la façon dont Data Protector sélectionne le jeu de supports si un même objet réside dans plusieurs jeux de supports.

Sélection des périphériques

Vous devez utiliser des périphériques distincts comme support source et support cible. Les périphériques cibles peuvent avoir une taille de bloc supérieure aux périphériques sources. Mais pour éviter de dégrader les performances, il est préférable que les périphériques aient la même taille de bloc et soient connectés au même système ou à un environnement SAN.

La charge de la copie d'objets est partagée par défaut. Data Protector exploite de façon optimale les périphériques disponibles en utilisant autant de périphériques que possible.

Si vous ne spécifiez pas les périphériques sources à utiliser dans la spécification de copie d'objets, Data Protector utilise les périphériques par défaut. Par défaut, les périphériques utilisés pour l'écriture des objets serviront de périphériques sources. Si nécessaire, vous pouvez modifier les périphériques sources. Si des périphériques cibles ne sont pas spécifiés par objet, Data Protector sélectionne automatiquement les périphériques les plus appropriés parmi ceux que vous avez sélectionnés dans la spécification de copie d'objets.

Les périphériques sont verrouillés au début de la session. Ceux qui ne sont pas disponibles à ce moment précis ne peuvent pas être utilisés durant la session car le verrouillage de périphérique est impossible après le début de la session. En cas d'erreur de support, le périphérique concerné sera évité pendant la session de copie.

Options de copie d'objets

Vous pouvez autoriser le filtrage d'objet source et indiquer la protection de données, la protection de catalogue et le niveau de connexion pour les copies d'objet dans la spécification de copie d'objet. Des équivalents de la plupart de ces options sont également utilisés pour la sauvegarde.

Selon votre stratégie, les objets sauvegardés et leurs copies peuvent avoir affiché des options identiques ou différentes. Par exemple, vous pouvez spécifier la valeur **Pas de journalisation** d'un objet de sauvegarde afin d'augmenter les performances de sauvegarde, puis spécifier la valeur **Journaliser tout** pour le même objet dans une session de copie d'objets ultérieure.

Pour créer des copies identiques d'objets sauvegardés, spécifiez le même niveau de journalisation pour les copies d'objets. Considérez que chaque copie d'objets avec un niveau de journalisation supérieur à Pas de journalisation a un impact sur la taille de l'IDB.

Sélection du jeu de supports comme source de la copie

Si une version d'objet que vous souhaitez copier existe sur plusieurs jeux de supports et a été créée en utilisant l'une des méthodes de déduplication de données Data Protector, n'importe quel jeu de supports peut servir de source pour la copie. Par défaut, Data Protector sélectionne automatiquement le jeu de supports qui sera utilisé. Vous pouvez influer sur cette sélection en spécifiant la priorité d'emplacement des supports.

Le processus global de sélection des supports est le même que pour la restauration. Lors d'une copie d'objets interactive, vous pouvez sélectionner manuellement le jeu de supports qui servira de source à la copie si votre point de départ est Objets ou Sessions. Lors de la configuration d'une copie d'objets

automatisée, vous ne pouvez pas sélectionner de supports car la sauvegarde des objets est souvent effectuée plus tard.

État d'achèvement d'une copie d'objets

Copie d'objets

Vous pouvez copier des objets qui ont le statut `Completed` ou `Completed/Errors`,, à condition que tous les supports sur lesquels ils se trouvent soient connectés à l'IDB. Si l'opération de copie est réussie, le statut de l'objet copié est le même que le statut de l'objet sauvegardé correspondant.

Si vous avez interrompu une session de copie d'objet ou si elle a échoué pour d'autres raisons, les copies d'objet qui résultent de cette session ont le statut `Failed`. Une copie d'objet ayant le statut `Failed` ne peut pas être copié à nouveau ; et ses données et son catalogue sont définis comme `None`.

Objets sources

Si une session de copie d'objets échoue, les objets sources qui ont été copiés restent inchangés.

Si une session de copie d'objets se termine avec des erreurs, les objets sources qui ont été copiés avec succès affichent des protections de données et de catalogue définies avec les valeurs spécifiées dans les options des objets sources.

Si vous interrompez une session de copie d'objet, la protection des données et du catalogue des objets source `all` demeure inchangée. Dans ce cas, si vous voulez modifier la protection de l'un des objets copiés, vous devez le faire manuellement dans l'IDB.

Propriété des copies d'objets

Le propriétaire des objets de sauvegarde copiés est le propriétaire des objets de sauvegarde originaux, non l'utilisateur Data Protector invoquant la session de copie d'objets.

Tâches de copie d'objets standard

Voici les conditions préalables et les limites de la fonction de copie d'objets :

Conditions préalables

- Vous devez installer un Agent de support sur chaque système qui participera à la session de copie d'objets.
- Vous devez également avoir au moins deux périphériques de sauvegarde configurés dans la cellule Data Protector.
- Vous devez préparer les supports pour la session de copie d'objets.
- Vous devez disposer des droits utilisateur appropriés pour démarrer une session de copie d'objets.

Limites

- Il n'est pas possible de copier des objets sauvegardés à l'aide de la fonction de sauvegarde ZDB sur disque ou NDMP.

- Il n'est pas possible de créer plusieurs copies d'une version d'objet dans une session de copie d'objets.
- Les périphériques cibles doivent avoir une taille de bloc égale ou supérieure à celle du périphérique source.
- Un même support ne peut pas être utilisé comme support source et support cible dans la même session de copie d'objets.
- Durant la copie d'objets, les supports utilisés comme sources ne sont pas disponibles pour la restauration.
- Il n'est pas possible de démultiplexer des objets d'intégration SAP MaxDB, DB2 UDB ou SQL.
- Il n'est pas possible de copier des objets sauvegardés, copiés ou consolidés pendant des sessions qui avaient été exécutées de façon interactive à partir de la dernière page de l'assistant.
- Il n'est pas possible de démarrer en parallèle deux ou plusieurs sessions de copie d'objets à partir de la même spécification de copie d'objets.

IMPORTANT :
Prenez en compte ce qui suit :

- Les intégrations Data Protector SAP MaxDB, DB2 UDB et Microsoft SQL Server possèdent des flux de données interdépendants. L'opération de copie d'objets doit donc conserver la disposition des objets sur les supports pour permettre une restauration. Pour cela, sélectionnez pour la copie tous les objets de ces intégrations ayant le même ID de sauvegarde. Sinon, une restauration de la copie sera impossible.
- Le nombre minimum de périphériques nécessaires pour une copie d'objets d'intégration SAP MaxDB, DB2 UDB ou Microsoft SQL Server est égal au nombre de périphériques utilisés pour la sauvegarde. La simultanéité des périphériques utilisés pour la sauvegarde et la copie de ces objets doit être la même.
- Si vous sélectionnez l'option Modifier la protection des données et du catalogue après une copie réussie si vous copiez des objets dans le cadre d'une session de sauvegarde ZDB sur disque + bande, sachez qu'après la période que vous spécifiez, les objets sources peuvent être écrasés. Une fois les supports écrasés, la restauration instantanée pour cette sauvegarde à l'aide de l'interface graphique n'est plus possible.
- Si vous abandonnez une session de copie d'objets, les protections des données et du catalogue de tous les objets sources restent inchangées. Dans ce cas, si vous voulez modifier la protection de l'un des objets copiés, vous devez le faire manuellement dans l'IDB.

Copie interactive d'objets

Une fois qu'un objet a été sauvegardé, vous pouvez le copier sur un nouveau jeu de supports.

Vous pouvez sélectionner des objets en vue d'une copie interactive à partir du point de départ Supports, Objets ou Sessions, selon vos besoins. Vous ne pouvez pas enregistrer une spécification de copie d'objets interactive ; vous pouvez uniquement lancer une session de copie d'objets.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez l'élément **Copie**, puis **Copie d'objets**, et enfin

Interactive.

3. Cliquez sur **Supports**, **Objets** ou **Sessions** pour ouvrir l'assistant.
   - Si vous choisissez **Supports**, la liste des supports et des pools de supports apparaît.
   - Si vous cliquez sur **Objets**, la liste des types de données sauvegardées (système de fichiers, base de données, etc.) apparaît.
   - Si vous choisissez **Sessions**, la liste des sessions au cours desquelles des objets ont été écrits sur des supports apparaît.
4. Sélectionnez les objets à copier.

   Si vous avez sélectionné Sessions à l'étape précédente, vous pouvez cliquer avec le bouton droit sur un objet d'intégration puis cliquer sur **Sélectionner le jeu de sauvegarde** afin de sélectionner tous les objets d'intégration portant le même ID de sauvegarde.

   > **REMARQUE :**
   > À partir de Data Protector 10.00 pour les sauvegardes VMware, les disques de la machine virtuelle sont considérés comme des objets qui s'exécutent en parallèle. Les objets disque de la machine virtuelle sont listés mais désactivés dans la liste **Supports** pour connaître les disques de la machine virtuelle qui sont sauvegardés sur le support. L'opération de copie ou de vérification est effectuée sur les objets de la machine virtuelle et tous ses objets disque associés sont pris en compte en interne.
   >
   > À partir de Data Protector 10.00 pour l'intégration VMware, l'option **Suivant** est activée uniquement après la sélection de l'objet de la machine virtuelle dans la liste **Supports**.

   Cliquez sur **Suivant**.
5. Les périphériques utilisés pour l'écriture des objets sélectionnés sont utilisés par défaut comme périphériques sources pour l'opération de copie d'objets. Si nécessaire, vous pouvez modifier les périphériques sources dans cette fenêtre. Sélectionnez le périphérique d'origine, puis cliquez sur **Modifier**. Le nom du nouveau périphérique apparaît sous Etat du périphérique. Ce nouveau périphérique ne servira que pour cette session.

   Pour obtenir des informations sur le périphérique, cliquez dessus avec le bouton droit, puis cliquez sur **Infos**.

   Indiquez l'opération que Data Protector doit effectuer si les périphériques sélectionnés ne sont pas disponibles pour la copie d'objets (s'ils sont, par exemple, désactivés ou en cours d'utilisation). Sélectionnez Sélection auto du périphérique ou Sélection du périphérique d'origine.

   Cliquez sur **Suivant**.
6. Sélectionnez les périphériques cibles pour l'opération de copie d'objets.

   Vous pouvez indiquer des périphériques pour chaque objet de la page Résumé à partir de la liste des périphériques spécifiés ici. Si vous ne spécifiez pas un périphérique pour chaque objet, Data Protector sélectionne les périphériques les plus adaptés à partir de cette liste.

   Cliquez sur **Suivant**.
7. Spécifiez les options d'objet source, d'objet cible et de support cible conformément à vos besoins. Cliquez sur **Suivant**.

Vous pouvez également sélectionner Utiliser la réplication pour effectuer une réplication entre deux périphériques B2D au lieu d'une copie. Une fois que Utiliser la réplication est sélectionné, la réplication vers une cellule étrangère est activée.

8. La liste des supports contenant les objets sélectionnés s'affiche.

   Si votre point de départ était Objets ou Sessions, la priorité d'emplacement des supports est également indiquée. Lorsqu'un même objet réside sur plusieurs jeux de supports, vous pouvez modifier la priorité d'emplacement des supports pour influer sur leur sélection.

   Cliquez sur **Suivant**.

9. Consultez le résumé des objets sélectionnés. Pour modifier des options pour un objet en particulier, sélectionnez-le dans la liste et cliquez sur **Propriétés**.

   Vous pouvez spécifier des options d'objet source et d'objet cible, ainsi que le périphérique cible. Si le point de départ Objets ou Sessions a été utilisé, vous pouvez sélectionner manuellement la copie de la version d'objet à utiliser s'il existe plusieurs copies.

10. Cliquez sur **Terminer** pour lancer l'assistant de copie.

Configuration de la copie d'objets post-sauvegarde

La copie d'objets post-sauvegarde s'effectue après l'achèvement d'une session de sauvegarde, session de copie d'objets ou session de consolidation d'objets définie sous le nom de la spécification de sauvegarde, de copie d'objets ou de consolidation d'objets dans la spécification de copie d'objets automatisée. Elle copie les objets créés au cours de la session qui correspondent aux critères spécifiés.

La session de copie d'objets post-sauvegarde ne démarre pas si la session de sauvegarde a échoué. Si la session de sauvegarde n'a pas été terminée, mais contient des objets sauvegardés, une session de copie d'objets post-sauvegarde copie les objets sauvegardés par défaut. Pour désactiver le processus de copie des sessions non terminées, attribuez la valeur 0 à l'option globale `CopyStartPostBackupOnAbortedSession`.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez l'élément **Copie**, puis **Copie d'objets**, et enfin **Automatisée**.
3. Cliquez sur **Post-sauvegarde** avec le bouton droit de la souris, puis cliquez sur **Ajouter** pour ouvrir l'assistant.
4. Sélectionnez les spécifications de sauvegarde, de copie d'objets ou de consolidation d'objet qui contiennent les objets à copier. Cliquez sur **Suivant**.
5. Spécifiez le filtre d'objets pour l'opération de copie d'objets. Seuls les objets répondant aux critères spécifiés seront copiés. Cliquez sur **Suivant**.
6. Spécifiez le filtre de bibliothèques pour l'opération de copie d'objets. Seuls les objets résidant sur des supports figurant dans les bibliothèques spécifiées seront copiés. Cliquez sur **Suivant**.
7. Les périphériques utilisés pour la sauvegarde dans les spécifications de sauvegarde sélectionnées sont utilisés par défaut comme périphériques sources pour l'opération de copie d'objets. Si nécessaire, vous pouvez modifier les périphériques sources dans cette fenêtre. Cliquez sur **Suivant**.

8. Sélectionnez les périphériques cibles pour l'opération de copie d'objets. Data Protector sélectionne les périphériques les plus adaptés à partir de ceux que vous indiquez ici. Cliquez sur **Next**.
9. Spécifiez les options d'objet source, d'objet cible et de support cible conformément à vos besoins. Cliquez sur **Suivant**.

   Vous pouvez également sélectionner Utiliser la réplication pour effectuer une réplication entre deux périphériques B2D au lieu d'une copie.
10. Cliquez sur **Enregistrer sous...**, saisissez un nom de spécification et cliquez sur **OK** pour enregistrer la spécification de copie d'objets post-sauvegarde.

Copie d'objets planifiée

La copie d'objets planifiée a lieu à l'heure définie par l'utilisateur. Les objets de différentes sessions de sauvegarde, de copie d'objets ou de consolidation d'objets peuvent être copiés au cours d'une même session de copie d'objets planifiée.

> **CONSEIL :**
> Vous pouvez également planifier des sessions de copie d'objets avec paramètres avancés avec le Planificateur basé sur Internet. Pour accéder au Planificateur, dans la liste de contexte, cliquez sur **Accueil**, puis sur **Planificateur** dans le volet de gauche.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez l'élément **Copie**, puis **Copie d'objets**, et enfin **Automatisée**.
3. Cliquez sur **Planifiée** avec le bouton droit de la souris, puis cliquez sur **Ajouter** pour ouvrir l'assistant.
4. Sélectionnez les spécifications de sauvegarde, de copie d'objets ou de consolidation d'objet qui contiennent les objets à copier.

   Vous pouvez également afficher les spécifications de sauvegarde par groupe de sauvegarde. Ainsi, si vous ajoutez une spécification de sauvegarde à un groupe de sauvegarde ou en supprimez une de ce groupe, la fonction de copie d'objets reconnaît automatiquement le changement et vous n'avez pas besoin de modifier manuellement la spécification de copie d'objets.

   Notez que si vous passez de la vue groupe à une autre vue, un message d'avertissement indique que le changement de vue supprimera toutes les sélections en cours. Si vous poursuivez, toutes les sélections antérieures sont effacées.

   Cliquez sur **Suivant**.
5. Spécifiez le filtre d'objets pour l'opération de copie d'objets. Seuls les objets répondant aux critères spécifiés seront copiés. Cliquez sur **Suivant**.
6. Spécifiez le filtre de bibliothèques pour l'opération de copie d'objets. Seuls les objets résidant sur des supports figurant dans les bibliothèques spécifiées seront copiés. Cliquez sur **Suivant**.
7. Les périphériques utilisés pour la sauvegarde dans les spécifications de sauvegarde sélectionnées sont utilisés par défaut comme périphériques sources pour l'opération de copie

d'objets. Si nécessaire, vous pouvez modifier les périphériques sources dans cette fenêtre. Cliquez sur **Suivant**.

8. Sélectionnez les périphériques cibles pour l'opération de copie d'objets. Data Protector sélectionne les périphériques les plus adaptés à partir de ceux que vous indiquez ici. Cliquez sur **Suivant**.
9. Spécifiez les options d'objet source, d'objet cible et de support cible conformément à vos besoins. Cliquez sur **Suivant**.

   Vous pouvez également sélectionner Utiliser la réplication pour effectuer une réplication entre deux périphériques B2D au lieu d'une copie.
10. Cliquez sur **Enregistrer et planifier...** Entrez un nom de spécification, puis cliquez sur **OK** pour enregistrer la spécification de copie d'objet planifiée. Une fois la spécification enregistrée, l'assistant de planification s'ouvre. Suivez les étapes de l'assistant pour planifier la spécification.

    Pour plus d'informations sur la création et la modification de planifications dans Data Protector à l'aide du planificateur, consultez la rubrique *Planificateur, Page 110*.

Redémarrage des sessions de copie d'objet ayant échoué

Du fait de problèmes de réseau ou de l'indisponibilité des systèmes, il peut arriver que certains objets échouent lors d'une session de copie d'objet. Vous pouvez relancer une session avec des erreurs après avoir résolu les problèmes imminents. Cette action ne redémarre que les objets ayant échoué.

Conditions préalables

- Vous devez être membre du groupe d'utilisateurs Admin Data Protector ou disposer des droits utilisateur Moniteur Data Protector.

Limites

- Vous ne pouvez pas redémarrer des sessions ayant échoué après avoir été exécutées de façon interactive, ce qui signifie qu'elles reposent sur des spécifications de copie d'objet non enregistrées.
- Il n'est pas possible de redémarrer plusieurs sessions simultanément.

> **IMPORTANT :**
> Ne modifiez pas une spécification de copie d'objet avant de redémarrer une session de copie d'objet ayant échoué. En effet, il ne serait pas possible de redémarrer tous les objets.

Procédure

1. Si vous utilisez un Gestionnaire de cellule ordinaire, cliquez sur **Base de données interne** dans la liste de contexte.

   Si vous utilisez les Gestionnaires MoM (Manager-of-Managers), choisissez **Clients** dans la liste de contexte, puis développez **Clients d'entreprise**. Sélectionnez un Gestionnaire de cellule rencontrant un problème de session. Dans le menu Outils, sélectionnez **Administration base de données** pour ouvrir une nouvelle fenêtre d'interface utilisateur Data Protector dans laquelle apparaît le contexte de la base de données interne.
2. Dans la fenêtre de navigation, développez **Base de données interne**, puis cliquez sur **Sessions**.

Une liste de sessions s'affiche dans la zone de résultats. L'état de chaque session est indiqué dans la colonne Etat.

3. Cliquez avec le bouton droit de la souris sur une session ayant échouée, abandonnée, ou encore une session s'étant achevée avec des échecs ou des erreurs, puis sélectionnez **Redémarrer objets ayant échoué** pour copier les objets ayant échoué.
4. Cliquez sur **Oui** pour confirmer.

Copie d'une spécification de copie d'objet

Vous pouvez copier une spécification de copie d'objets déjà configurée et enregistrée.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez **Copie**, **Copie d'objet**, **Automatisée**, puis **Post sauvegarde**. Toutes les spécifications de copie d'objets enregistrées s'affichent alors.
3. Dans la zone de résultats, cliquez avec le bouton droit sur la spécification de copie d'objet à copier, puis cliquez sur **Copier sous**. La boîte de dialogue Copier sous s'affiche.
4. Dans la zone de texte Nom, attribuez un nom à la spécification de copie d'objets copiée.
5. Cliquez sur **OK**.

La spécification de copie d'objets copiée s'affiche dans le contexte des opérations sur les objets de la fenêtre de navigation ainsi que dans la zone de résultats sous son nouveau nom.

Tâches de copie d'objets avancées

Des copies de données sauvegardées sont créées à différentes fins :

- Mise au coffre

  Vous pouvez faire des copies d'objets sauvegardés, copiés ou consolidés et les stocker à plusieurs emplacements.
- Libération de supports

  Pour ne conserver que des versions d'objet protégées sur des supports, vous pouvez copier ces versions d'objet, puis libérer le support à des fins d'écrasement.
- Démultiplexage de supports

  Vous pouvez copier des objets pour éliminer l'entrelacement de données.
- Consolidation d'une chaîne de restauration

  Vous pouvez copier toutes les versions de l'objet nécessaires pour une restauration vers un ensemble de supports.
- Migration vers un autre de type de support

  Vous pouvez copier vos sauvegardes sur des supports d'un autre type.
- Prise en charge de concepts de sauvegarde avancés

  Vous pouvez utiliser des concepts de sauvegarde tels que la sauvegarde de disque en plusieurs étapes.

Libération d'un support

Un support peut contenir des objets sauvegardés avec des périodes de protection différentes. Il se peut que seule une petite partie de l'espace sur le support soit occupée par un objet protégé. Cependant, vous ne pouvez pas réutiliser ce support tant que la période de protection de tous les objets n'est pas terminée.

Pour rationaliser l'utilisation des supports, vous pouvez libérer ceux qui contiennent seulement quelques objets protégés à l'aide de la fonction de copie d'objets. Les objets protégés sont copiés sur un nouveau jeu de supports et le support peut être réutilisé. Vous pouvez également libérer des supports attachés à des objets ayant échoué. Ces objets ne sont pas copiés lors de la session de copie d'objets.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez l'élément **Copie**, puis **Copie d'objets**, et enfin **Interactive**.
3. Cliquez sur **Support** pour ouvrir l'assistant.
4. Sur la page Objets, sélectionnez l'option Permettre la sélection des objets protégés uniquement. Développez les pools de supports et sélectionnez les supports que vous souhaitez libérer. Cliquez sur **Next**.
5. Les périphériques utilisés pour l'écriture des objets sélectionnés sont utilisés par défaut comme périphériques sources pour l'opération de copie d'objets. Si nécessaire, vous pouvez modifier les périphériques sources dans cette fenêtre. Cliquez sur **Next**.
6. Sélectionnez les périphériques cibles pour l'opération de copie d'objets.

   Vous pouvez indiquer des périphériques pour chaque objet de la page Résumé à partir de la liste des périphériques spécifiés ici. Si vous ne spécifiez pas un périphérique pour chaque objet, Data Protector sélectionne les périphériques les plus adaptés à partir de cette liste.

   Cliquez sur **Next**.
7. Dans la page Options, sous Options pour l'objet source, sélectionnez l'option Modifier la protection des données et du catalogue après une copie réussie pour enlever la protection des objets sources une fois ceux-ci copiés. Sélectionnez Recycler les données et la protection de catalogue des objets sources ayant échoué après une copie réussie afin d'enlever la protection de ces objets (ceux-ci ne seront pas copiés). Spécifiez d'autres options si nécessaire. Cliquez sur **Next**.
8. La liste des supports contenant les objets sélectionnés s'affiche. Cliquez sur **Next**.
9. Consultez le résumé des objets sélectionnés. Pour modifier des options pour un objet en particulier, sélectionnez-le dans la liste et cliquez sur **Propriétés**. Vous pouvez spécifier des options d'objet source et d'objet cible, ainsi que le périphérique cible.
10. Cliquez sur **Terminer** pour lancer la session de copie.

Démultiplexage d'un support

Les supports multiplexés peuvent contenir des données entrelacées de plusieurs objets. Ces supports peuvent résulter de sessions de sauvegarde avec plusieurs périphériques fonctionnant simultanément. Ils peuvent compromettre la confidentialité des sauvegardes et leur restauration peut durer plus longtemps.

La fonction de copie d'objets vous permet de démultiplexer des supports. Les objets issus d'un support multiplexé sont copiés vers plusieurs supports.

Limite

Data Protector ne lit le support source qu'une seule fois. Pour que le démultiplexage de tous les objets sur le support soit possible, le nombre minimum de périphériques cibles requis pour cette opération doit être le même que le nombre défini pour la simultanéité de périphériques lors de l'écriture des objets. Si le nombre de périphériques disponibles est inférieur, certains objets seront encore multiplexés sur le support cible.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez l'élément **Copie**, puis **Copie d'objets**, et enfin **Interactive**.
3. Cliquez sur **Sessions** pour ouvrir l'assistant.
4. Développez les sessions de votre choix et sélectionnez les objets à copier. Cliquez sur **Suivant**.
5. Réalisez cette étape si vous ne voulez pas que l'opération de démultiplexage occupe le ou les périphériques configurés pour les sauvegardes normales et si vous souhaitez utiliser un seul périphérique pour la lecture des données lors de cette opération.

   Mappez le ou les périphériques sources en un seul périphérique.

   > **IMPORTANT :**
   > Ignorez cette étape si vous avez utilisé un périphérique de fichier autonome en tant que périphérique source. Si vous avez utilisé un périphérique de bibliothèque de stockage de fichiers ou un périphérique de bibliothèque de fichiers comme périphérique source, assurez-vous de mapper le ou les périphériques sources en périphériques dans la même bibliothèque de stockage de fichiers ou dans la même bibliothèque de fichiers.

   Cliquez avec le bouton droit sur chaque périphérique et sélectionnez **Changer périphérique**. Sélectionnez le nouveau périphérique, puis cliquez sur **OK**.
6. Cliquez sur **Suivant**.
7. Sélectionnez les périphériques cibles pour l'opération de copie d'objets. Le nombre de périphériques requis dépend de la simultanéité de périphériques utilisée lors de l'écriture des objets.

   Cliquez avec le bouton droit de la souris sur le lecteur sélectionné et cliquez sur **Propriétés**. Attribuez la valeur 1 à l'option **Simultanéité**. Cliquez sur **OK**.

Vous pouvez indiquer des périphériques pour chaque objet de la page Résumé à partir de la liste des périphériques spécifiés ici. Si vous ne spécifiez pas un périphérique pour chaque objet, Data Protector sélectionne les périphériques les plus adaptés à partir de cette liste.

Cliquez sur **Suivant**.

8. Spécifiez les options d'objet source, d'objet cible et de support cible conformément à vos besoins. Cliquez sur **Suivant**.
9. La liste des supports contenant les objets sélectionnés s'affiche.

   Lorsqu'un même objet réside sur plusieurs jeux de supports, vous pouvez modifier la priorité d'emplacement des supports pour influer sur leur sélection.

   Cliquez sur **Suivant**.
10. Consultez le résumé des objets sélectionnés. Pour modifier des options pour un objet en particulier, sélectionnez-le dans la liste et cliquez sur **Propriétés**.

    Vous pouvez spécifier des options d'objet source et d'objet cible, ainsi que le périphérique cible. Vous pouvez aussi sélectionner manuellement la copie de la version d'objet à utiliser s'il existe plusieurs copies.
11. Cliquez sur **Terminer** pour lancer l'assistant de copie.

Consolidation d'une chaîne de restauration

La fonction de copie d'objets vous permet de copier une chaîne de restauration d'une version d'objet sur un nouveau jeu de supports. Une restauration effectuée à partir de ce type de jeu de supports est plus rapide et plus pratique. En effet, il n'est pas nécessaire de charger plusieurs supports et de rechercher les versions d'objet nécessaires.

> **REMARQUE :**
> Data Protector offre une fonction encore plus puissante : consolidation d'objets. Alors que la copie d'objets vous permet de copier toutes les sauvegardes d'une chaîne de restauration dans une séquence, la consolidation d'objets fusionne les sauvegardes dans une nouvelle version d'objet, une sauvegarde complète synthétique.

Limite

La sélection d'une chaîne de restauration n'est pas disponible pour les objets d'intégration.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez l'élément **Copie**, puis **Copie d'objets**, et enfin **Interactive**.
3. Cliquez sur **Objets** pour ouvrir l'assistant.
4. Dans la page Objets, développez un type de donnée, puis un client et ses disques logiques ou points de montage pour afficher les versions d'objet. Cliquez avec le bouton droit de la souris sur les objets à copier et choisissez **Sélectionner une chaîne de restauration**. Cliquez sur **Suivant**.
5. Les périphériques utilisés pour l'écriture des objets sélectionnés sont utilisés par défaut comme périphériques sources pour l'opération de copie d'objets. Si nécessaire, vous pouvez modifier les

périphériques sources dans cette fenêtre. Cliquez sur **Suivant**.

6. Sélectionnez les périphériques cibles pour l'opération de copie d'objets.

   Vous pouvez indiquer des périphériques pour chaque objet de la page Résumé à partir de la liste des périphériques spécifiés ici. Si vous ne spécifiez pas un périphérique pour chaque objet, Data Protector sélectionne les périphériques les plus adaptés à partir de cette liste.

   Cliquez sur **Suivant**.
7. Spécifiez les options d'objet source, d'objet cible et de support cible conformément à vos besoins. Cliquez sur **Suivant**.
8. La liste des supports contenant les objets sélectionnés s'affiche.

   Lorsqu'un même objet réside sur plusieurs jeux de supports, vous pouvez modifier la priorité d'emplacement des supports pour influer sur leur sélection.

   Cliquez sur **Suivant**.
9. Consultez le résumé des objets sélectionnés. Pour modifier des options pour un objet en particulier, sélectionnez-le dans la liste et cliquez sur **Propriétés**.

   Vous pouvez spécifier des options d'objet source et d'objet cible, ainsi que le périphérique cible. Vous pouvez aussi sélectionner manuellement la copie de la version d'objet à utiliser s'il existe plusieurs copies.
10. Cliquez sur **Terminer** pour lancer l'assistant de copie.

Migration vers un autre type de support

Vous pouvez utiliser la fonction de copie d'objets pour migrer les données sauvegardées vers un autre type de support avec une taille de bloc identique ou supérieure.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez l'élément **Copie**, puis **Copie d'objets**, et enfin **Interactive**.
3. Cliquez sur **Support** pour ouvrir l'assistant.
4. Sélectionnez les objets à copier et cliquez sur **Suivant**.
5. Les périphériques utilisés pour l'écriture des objets sélectionnés sont utilisés par défaut comme périphériques sources pour l'opération de copie d'objets. Si nécessaire, vous pouvez modifier les périphériques sources dans cette fenêtre. Cliquez sur **Suivant**.
6. Sélectionnez les périphériques cibles pour l'opération de copie d'objets.

   Vous pouvez indiquer des périphériques pour chaque objet de la page Résumé à partir de la liste des périphériques spécifiés ici. Si vous ne spécifiez pas un périphérique pour chaque objet, Data Protector sélectionne les périphériques les plus adaptés à partir de cette liste.

   Cliquez sur **Suivant**.
7. Spécifiez les options d'objet source, d'objet cible et de support cible conformément à vos besoins. Cliquez sur **Suivant**.
8. La liste des supports contenant les objets sélectionnés s'affiche. Cliquez sur **Suivant**.
9. Consultez le résumé des objets sélectionnés. Pour modifier des options pour un objet en

particulier, sélectionnez-le dans la liste et cliquez sur **Propriétés**.

Vous pouvez spécifier des options d'objet source et d'objet cible, ainsi que le périphérique cible.

10. Cliquez sur **Terminer** pour lancer l'assistant de copie.

À propos de la sauvegarde de disque en plusieurs étapes

Qu'est-ce que la sauvegarde de disque en plusieurs étapes ?

La sauvegarde de disque en plusieurs étapes consiste à sauvegarder des données à plusieurs reprises. La procédure consiste à sauvegarder les données sur un support d'un type, puis à les copier par la suite vers un support d'un autre type. Cette fonctionnalité s'utilise généralement comme suit

1. Les données sont sauvegardées sur un support très performant et très accessible, mais de faible capacité (par exemple, un disque système). Ces sauvegardes restent accessibles pendant la période de temps la plus susceptible de demander une restauration rapide.
2. Après un certain temps, les données sont transférées sur un support moins performant et moins accessible, mais de plus grande capacité, à l'aide de la fonction de copie d'objets.

Vous pouvez échelonner un disque de cette manière à l'aide de la spécification de copie d'objets configurée spécifiquement à cet effet.

Vous pouvez adopter l'alternative suivante:

1. Créer une spécification de sauvegarde indiquant de sauvegarder les données sur le support hautes performances après avoir défini la protection sur la période totale sur laquelle la fonction de restauration s'avère nécessaire.
2. Créer une spécification de copie post-sauvegarde automatisée afin de copier les données sauvegardées sur le support moins performant, puis redéfinir la période de rétention de la sauvegarde d'origine sur la période critique au cours de laquelle la fonction de restauration rapide s'avère nécessaire. Par défaut, la copie secondaire est conservée pendant la période de protection précisée dans la spécification de sauvegarde d'origine.

Cette méthode offre la sécurité supplémentaire de disposer des deux copies au cours de la période critique.

Avantages de la mise en œuvre de la sauvegarde de disque en plusieurs étapes

L'utilisation de la sauvegarde de disque en plusieurs étapes présente les avantages suivants :

- Meilleures performances lors des opérations de sauvegarde et de restauration
- Réduction des coûts de stockage des données sauvegardées
- Meilleures disponibilité et accessibilité des données en vue d'une restauration

Sauvegarde de disque en plusieurs étapes et petites sauvegardes récurrentes

La sauvegarde de disque en plusieurs étapes élimine également le besoin d'effectuer fréquemment des sauvegardes sur bande de nombreux objets de petite taille. Ce type de sauvegarde est peu pratique en

raison du chargement et du déchargement fréquents des supports. L'utilisation de la sauvegarde de disque en plusieurs étapes peut réduire la durée de sauvegarde et éviter la détérioration des supports.

Dépannage des sessions de copie d'objets

Problèmes de copie d'objets

Copie d'objets plus importante que prévu

Problème
Lors d'une copie d'objets planifiée ou après sauvegarde, le nombre d'objets correspondant aux filtres sélectionnés est supérieur au nombre d'objets effectivement copiés. Le message suivant s'affiche : `Too many objects match specified filters.`
Action
• Resserrez les critères de sélection de la version d'objet. • Augmentez le nombre maximal d'objets copiés dans une session en modifiant la valeur de l'option globale `CopyAutomatedMaxObjects`.

Tous les objets de la bibliothèque sélectionnée n'ont pas été copiés

Problème
Lors d'une copie d'objets planifiée ou après sauvegarde, certains objets résidant sur des supports de la bibliothèque sélectionnée ne sont pas copiés. Ceci se produit si un objet ne dispose pas d'un jeu de supports complet dans la bibliothèque sélectionnée.
Action
Insérez le support manquant dans la bibliothèque sélectionnée ou sélectionnez la bibliothèque qui dispose d'un jeu de supports complet pour ces objets.

Demande de montage pour supports supplémentaires

Problème
Lors d'une session de copie d'objet interactive à partir du point de départ, vous avez sélectionné un support spécifique. Une demande de montage pour supports supplémentaires a été émise. Ceci se produit si un objet résidant sur le support s'étend à un autre support.
Action
Insérez le support requis dans le périphérique et confirmez la demande de montage.

Lors de la création d'une copie d'objet, l'heure de fin de la protection a été prolongée

Problème
Lors de la création d'une copie d'objet, la date/heure de fin de la protection n'est pas héritée de l'objet d'origine. La longueur de la protection est copiée, mais la date de début est définie sur la date de création de la copie d'objets et pas sur la date de création de l'objet. Ceci permet d'augmenter le délai de protection de l'original. Plus longue est la durée entre la sauvegarde originale et la session de copie d'objets, plus importante sera la différence entre les dates de fin de la protection. Par exemple, si l'objet a été créé le 05 septembre, avec une protection définie sur 14 jours, la protection expirera le 19 septembre. Si la session de copie d'objet a débuté le 10 septembre, la protection de la copie d'objet expirera le 24 septembre. Dans certains cas, ceci n'est pas souhaitable et la date de fin de la protection prévue doit être maintenue.
Action
Définissez l'option globale `CopyDataProtectionEndtimeEqualToBackup` à `1`de manière à assurer que la date de fin de la protection de la copie d'objet soit égale à la date de fin de la protection de l'objet sauvegarde. Par défaut, cette option est définie sur 0. Augmentez le nombre maximum de fichiers autorisés.

La session de réplication d'objets multiples ne répond plus

Problème

Lors de la réplication d'une session vers un autre périphérique, la session ne répond plus. Les résultats de la session fournissent les informations suivantes :
`[Normal] From: BMA@company.com "d2d1_1_gw1 [GW 26177:1:15198446278003495809]" Time: 3/21/2013 9:13:06 AM`
`COMPLETED Media Agent "d2d1_1_gw1 [GW 26177:1:15198446278003495809]"`
Ce problème survient généralement dans des configurations réseau à double pile IP avec agent de support HP-UX.

Action

Lors de la configuration d'un réseau IP à double pile, ajoutez une entrée distincte pour les adresses d'hôte local IPv6 dans le fichier `/etc/hosts` du client Agent de support.
Par exemple, le fichier `hosts` comporte l'entrée suivante :
`::1 localhost loopback`
Pour résoudre le problème, ajoutez la ligne suivante aux adresses IPv6 :
`::1 ipv6-localhost ipv6-loopback`

Une session de réplication sur des périphériques d'amélioration du domaine de données ne répond pas à l'opération Abandonner lors de la période de nouvel essai

Problème
Lorsque la réplication d'une session d'un périphérique de sauvegarde d'amélioration du domaine de données à un autre n'a pas assez de flux disponibles, la session de réplication est incapable de répondre aux opérations Abandonner pendant la période de nouvel essai.
Action
Le problème se produit quand la variable `omnirc DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT` est définie sur `0`, ce qui n'est pas pris en charge. Cette variable définit le nombre de secondes d'attente de la session de réplication avant de lancer un nouvel essai lorsque le périphérique d'amélioration du domaine de données n'a pas assez de flux disponibles. Si l'intervalle est trop grand ou défini sur `0`, la session ne pourra pas répondre aux opérations Abandonner. La valeur par défaut pour `DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT` est de 60 secondes. Voir le fichier `omnirc` pour une description complète de `DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT`.

Problèmes de consolidation d'objets

La consolidation d'objets à des stades différents ouvre un trop grand nombre de fichiers

Problème

Si vous lancez une opération de consolidation d'objets à des stades différents, Data Protector lit tous les supports nécessaires au bon déroulement de l'opération. Cette opération entraîne l'ouverture simultanée de tous les fichiers. Lorsque Data Protector ouvre un plus grand nombre de fichiers que le nombre autorisé par votre système d'exploitation, un message similaire au suivant s'affiche :
`|Major| From: RMA@computer.company.com "AFL1_ConsolidateConc2_bs128" Time: time /omni/temp/Cons_Media/AFL1/`
`0a1109ab54417fab351d15500c6.fd`
`Cannot open device ([24] Too many open files)`

Action
Augmentez le nombre maximum de fichiers autorisés. **Systèmes HP-UX :**

1. Définissez le nombre maximum de fichiers ouverts avec SAM (System Administration Manager) :
   a. Sélectionnez **Kernel Configuration > Configurable parameters** puis, **Actions** > **Modify Configurable Parameter**.
   b. Entrez les nouvelles valeurs **maxfiles_lim** et **maxfiles** dans le champ **formula/value**.
2. Redémarrez votre ordinateur après avoir appliqué les nouvelles valeurs.

Systèmes Solaris :

1. Définissez le nombre maximum de fichiers ouverts en éditant le fichier `/etc/system`. Ajoutez les lignes suivantes :

   ```
   set rlim_fd_cur=value
   set rlim_fd_max=value
   ```

2. Redémarrez votre ordinateur après avoir appliqué les nouvelles valeurs.

La consolidation d'objets sur des périphériques B2D a échoué à la seconde tentative

Problème
Après la première consolidation d'objet, si vous procédez à une sauvegarde incrémentale puis que vous tentez d'effectuer une seconde consolidation d'objet, l'opération échouera.
Action
Pour garantir la réussite de la seconde consolidation, exécutez une sauvegarde complète après la première consolidation d'objet. Lancez ensuite une sauvegarde incrémentale, qui pourra être consolidée par la suite.

À propos de la réplication

La fonction de réplication Data Protector vous permet de répliquer des objets entre deux périphériques de sauvegarde sur disque (B2D) capables de réplication, sans transférer les données par l'intermédiaire d'Agents de support. Vous pouvez sélectionner une session de sauvegarde, de copie ou de consolidation d'objets. Au cours de la session de réplication, Data Protector lit l'objet de la session en cours de réplication et lance la réplication du périphérique B2D source vers le périphérique cible.

Le résultat d'une session de réplication est une copie de tous les objets de la session que vous aurez spécifiés.

Voici les caractéristiques de la fonction de réplication :

- Démarrage de la session

  Une session de réplication peut être démarrée de manière interactive ou automatique.
- Sélection des périphériques cibles

  Vous pouvez filtrer les périphériques permettant la réplication et sélectionner un périphérique adapté.
- Stratégie de protection

Vous pouvez définir de façon indépendante les périodes de protection des objets sources et des copies d'objets.

Vous pouvez lancer une session de réplication de manière interactive ou spécifier un démarrage automatisé de la session.

Réplication automatisée

Une spécification de réplication automatisée consiste à définir un ou plusieurs critères pour la sélection des versions d'objet à copier :

- Spécifications de sauvegarde - pour ne copier que des versions d'objet sauvegardées au moyen de certaines spécifications.
- Spécifications de copie d'objets - pour ne copier que les versions d'objets copiées au moyen de spécifications de copie d'objets spécifiques.
- Spécifications de consolidation d'objets - pour ne copier que les versions d'objets consolidées au moyen de spécifications de consolidation d'objets spécifiques.
- Protection des données - pour ne copier que des versions d'objets protégées.
- Nombre de copies existantes - pour ne copier que les versions d'objet ne comportant pas plus que le nombre de copies réussies indiqué.
- Bibliothèques - pour ne copier que les versions d'objet se trouvant sur les supports des bibliothèques indiquées.
- Période (uniquement en cas de spécification de copie d'objets planifiée) - pour ne copier que des versions d'objet sauvegardées dans la période indiquée.

Data Protector offre deux types de réplication automatisée : réplication post-sauvegarde et réplication planifiée.

Réplication post-sauvegarde

La réplication post-sauvegarde, post-copie et post-consolidation (sous-ensembles de la réplication post-sauvegarde), s'effectue après l'achèvement d'une session spécifiée dans la spécification de copie d'objets automatique. Elle copie les objets sélectionnés en fonction de la spécification de réplication automatisée, qui ont été écrits au cours de la session concernée.

réplication planifiée

La réplication planifiée a lieu à l'heure définie par l'utilisateur. Les objets de différentes sessions peuvent être répliqués au cours d'une même session de réplication planifiée.

Limites

- Vous pouvez uniquement sélectionner des sessions de sauvegarde, de copie, de consolidation ou de réplication d'objets pour la réplication. La sélection d'objets individuels n'est pas prise en charge.
- Les tailles de blocs différentes sur le périphérique source ou cible ne sont pas prises en charge.
- Lors de la configuration de sessions interactives, vous ne pouvez sélectionner qu'une session à la fois.

Points à prendre en considération

- Comme la réplication est basée sur une session, les paramètres des objets individuels peuvent être remplacés. Par exemple, si vous avez déjà un certain nombre de copies d'un objet dans la session, Data Protector ignore l'option **Inclure uniquement les objets avec nombre de copies inférieur à** et réplique tous les objets de la session, y compris cet objet, même si cela aboutit au fait que l'objet comporte plus de copies que cela n'est autorisé avec cette option.
- Par défaut, Data Protector sélectionne la version originale de l'objet (s'il existe plusieurs copies d'un même objet) comme périphérique source. Dans certaines circonstances, la version originale peut ne pas permettre la réplication car son type de support est différent.

  Sélectionnez le périphérique source correct en choisissant la bibliothèque permettant la réplication ou sélectionnez la bibliothèque spécifique.

Activation de la réplication

Vous pouvez activer la réplication d'un périphérique B2D vers l'autre *lorsque vous créez une spécification de copie d'objets* :

1. Assurez-vous que les périphériques sources et cibles permettent la réplication. Utilisez le filtre **Permet la réplication** pour filtrer les périphériques, ou sélectionnez explicitement les périphériques B2D spécifiques.
2. Lors du réglage des options de l'opération de copie, sélectionnez **Utiliser la réplication**.

Pour connaître la procédure détaillée, consultez les tâches de copie d'objets standard.

Synchronisation automatisée de réplication

La fonction de réplication de Data Protector vous permet de répliquer des objets entre deux périphériques de sauvegarde sur disque (B2D) capables de réplication, sans transférer les données par l'intermédiaire d'Agents de support. La fonction de synchronisation automatisée de réplique est une extension de la réplication normale, qui vous permet de répliquer les métadonnées de sauvegarde entre deux appareils de déduplication gérés par des Gestionnaires de cellule différents. Cette fonction vous permet d’échanger facilement des données de sauvegarde et d’autres métadonnées entre deux appareils de déduplication.

Conditions préalables

Assurez-vous que l’utilisateur Data Protector (sous le compte duquel le CRS est exécuté) dans le Gestionnaire de cellule source dispose d’un accès au Gestionnaire de cellule cible.

Points à prendre en considération

Pour les sauvegardes d’intégration, n’exécutez pas la procédure de synchronisation automatisée de réplique à partir de sessions de sauvegarde ayant partiellement échoué (sessions de sauvegarde terminées avec des erreurs). La réplication aboutira, mais la restauration à partir de la session répliquée risque d’échouer.

Limites

- Prenez en considération toutes les limitations qui s'appliquent à la fonction de réplication normale.
- La version du Gestionnaire de cellule cible doit être identique ou plus récente que celle du Gestionnaire de cellule source.
- Les périphériques dans le Gestionnaire de cellule source et le Gestionnaire de cellule étranger (gestionnaire de cellule cible), qui sont sélectionnés pour la réplication, doivent pointer vers le même périphérique physique et la même banque de données.
- Le nombre maximum de supports susceptibles d'être répliqués simultanément dépend des connexions libres disponibles sur le périphérique cible. Par exemple, si le périphérique cible dispose de 100 connexions libres, il est recommandé qu'au plus 100 supports peuvent être répliqués simultanément. De même, si vous souhaitez utiliser le périphérique cible pour d'autres opérations, le nombre de supports susceptibles d'être répliqués simultanément doit être inférieur au nombre de connexions libres disponibles.

  Pour les périphériques StoreOnce et Data Domain Boost, vérifiez respectivement les connexions de données et les flux de réplication disponibles. Pour plus d'informations sur les flux pris en charge, consultez les manuels des périphériques correspondants.
- La génération de la liste Synchronisation automatisée de réplique à l'aide d'une interface utilisateur graphique de version antérieure n'est pas prise en charge. Le message d'erreur suivant peut s'afficher : « `Error parsing Copy Specification file. The file may be corrupted or invalid.` » Ce message indique que l'interface utilisateur graphique Data Protector des versions antérieures ne prend pas en charge la nouvelle liste.
- L'option **Inclure uniquement les objets avec nombre de copies inférieur à** n'est pas prise en charge pour la procédure de synchronisation automatisée de réplique.

La synchronisation automatisée de réplique implique deux procédures :

1. Importation du Gestionnaire de cellule étranger
2. Exécution d'une session de copie d'objets

Importation du Gestionnaire de cellule étranger

La première étape de déclenchement de la synchronisation automatisée de réplique consiste à importer le Gestionnaire de cellule étranger dans le Gestionnaire de cellule source. Pour importer le Gestionnaire de cellule étranger :

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. Saisissez le nom du client ou naviguez sur le réseau pour sélectionner le client (dans l'interface client Windows uniquement) à importer. Si vous importez un Gestionnaire de cellule qui gère un appareil de déduplication, sélectionnez **Serveur de cellule étranger Data Protector**

   > **REMARQUE :** l'étape ci-dessus est pertinente si vous exécutez la procédure de synchronisation automatisée de réplication.

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

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

> **REMARQUE :** vous pouvez uniquement exécuter l'opération de synchronisation automatisée sur le Gestionnaire de cellule importé. Aucune autre opération ne pourra être exécutée en utilisant le Gestionnaire de cellule.

Exécution d'une session de copie d'objets

Après l'importation du Gestionnaire de cellule étranger à la source Gestionnaire de cellule, vous pouvez exécuter une session de copie d'objets pour copier les données de sauvegarde et les autre méta données dans le Gestionnaire de cellule étrangère. Vous pouvez effectuer une copie d'objets interactive, post-sauvegarde ou planifiée selon vos besoins.

Pour exécuter une session de copie d'objets :

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, accédez à **Copier** > **Copie d'objets** > **Automatisée**.
3. Cliquez sur **Planifiée** avec le bouton droit de la souris, puis cliquez sur **Ajouter** pour ouvrir l'assistant. Vous pouvez également effectuer une session de copie d'objets interactive ou post-sauvegarde.
4. Sélectionnez les spécifications de sauvegarde, de copie d'objets ou de consolidation d'objet qui contiennent les objets à copier. Cliquez sur **Suivant**.
5. Spécifiez le filtre d'objets pour l'opération de copie d'objets. Seuls les objets répondant aux critères spécifiés seront copiés. Cliquez sur **Suivant**.
6. Spécifiez le filtre de bibliothèques pour l'opération de copie d'objets. Seuls les objets résidant sur des supports figurant dans les bibliothèques spécifiées seront copiés. Cliquez sur **Suivant**.
7. Les périphériques utilisés pour la sauvegarde dans les spécifications de sauvegarde sélectionnées sont utilisés par défaut comme périphériques sources pour l'opération de copie d'objets. Si nécessaire, vous pouvez modifier les périphériques sources dans cette fenêtre. Cliquez sur **Suivant**.
8. Sélectionnez les périphériques cibles pour l'opération de copie d'objets. Data Protector sélectionne les périphériques les plus adaptés à partir de ceux que vous indiquez ici. Cliquez sur **Suivant**.

   Cochez la case **Afficher capable de réplication** pour sélectionner uniquement les périphériques possédant des périphériques (de déduplication) de sauvegarde sur disque. La réplication est possible uniquement sur les périphériques de sauvegarde sur disque.
9. Spécifiez les options d'objet source, d'objet cible et de support cible conformément à vos besoins.

   Sélectionnez **Utiliser la réplication** pour effectuer une réplication entre deux périphériques B2D au lieu d'une copie.

   Sélectionnez **Répliquer dans cellule étrangère** pour activer la réplication d'objets vers le serveur de cellule étranger que vous avez importé précédemment (ce Gestionnaire de cellule comporte le deuxième périphérique de déduplication).

   Cliquez sur **Suivant**.
10. Sélectionnez le serveur de cellule étranger que vous avez importé précédemment à partir du menu déroulant. Celui-ci fournit la liste des périphériques qui sont liés à la banque de sauvegarde sur disque.

Tous les périphériques créés à partir du Gestionnaire de cellule cible et qui sont associés au même nom de banque sont affichés ici. Par conséquent, vous devez veiller à sélectionner le périphérique associé au nom de banque correct pour la réplication.

Sélectionnez la passerelle ou le périphérique requis, puis cliquez sur **Suivant**.

11. Cliquez sur **Enregistrer et planifier...** Entrez un nom de spécification, puis cliquez sur **OK** pour enregistrer la spécification de copie d'objet planifiée. Une fois la spécification enregistrée, l'assistant de planification s'ouvre. Suivez les étapes de l'assistant pour planifier la spécification.

    Pour plus d'informations sur la création et la modification de planifications dans Data Protector à l'aide du planificateur, consultez la rubrique *Planificateur, Page 110*.

Exécutez la session de copie d'objets pour terminer la procédure de resynchronisation automatisée de réplique.

À propos de la mise en miroir d'objets

La fonctionnalité de mise en miroir d'objets de Data Protector permet l'écriture simultanée des mêmes données sur plusieurs jeux de supports au cours d'une session de sauvegarde. Vous pouvez mettre en miroir tout ou partie des objets sauvegarde sur un ou plusieurs jeux de supports supplémentaires.

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

Avantages de la copie par symétrie

L'utilisation de la fonctionnalité miroir d'objet répond aux objectifs suivants :

- Elle accroît la disponibilité de données sauvegardées du fait de l'existence de copies multiples.
- Elle permet une mise au coffre multi-site simplifiée, alors que les données sauvegardées peuvent être copiées par symétrie vers des sites éloignés.
- Elle améliore la tolérance aux pannes des sauvegardes car les mêmes données sont écrites sur plusieurs supports. Une panne de disque sur un support n'a pas d'incidence sur la création des autres miroirs.

Limites

- Il n'est pas possible de mettre en miroir des objets sauvegardés à l'aide de la fonction de sauvegarde ZDB sur disque ou NDMP.
- Il n'est pas possible de mettre en miroir un objet sur le même périphérique plus d'une fois dans une même session.
- La taille de bloc des périphériques ne doit pas diminuer au sein d'une chaîne de miroirs. Cela signifie que :
  - les périphériques utilisés pour l'écriture du miroir 1 doivent avoir une taille de bloc identique ou supérieure à celle des périphériques utilisés pour la sauvegarde ;
  - les périphériques utilisés pour l'écriture du miroir 2 doivent avoir une taille de bloc identique ou supérieure à celle des périphériques utilisés pour l'écriture du miroir 1, etc.

Comment utiliser la mise en miroir d'objet

Vous spécifiez une mise en miroir d'objet lors de la configuration d'une spécification de sauvegarde. Dans la spécification de sauvegarde, sélectionnez les objets que vous souhaitez mettre en miroir, puis indiquez le nombre de miroirs. Pour spécifier plus de 5 miroirs, augmentez la valeur de l'option globale `MaxNumberOfMirrors`.

Spécifiez des périphériques séparés pour la sauvegarde et pour chaque miroir. Lorsqu'une session de sauvegarde avec mise en miroir d'objet commence, Data Protector sélectionne les périphériques parmi ceux que vous avez indiqués dans la spécification de sauvegarde. Pour éviter de dégrader les performances, il est préférable que les périphériques aient la même taille de bloc et soient connectés au même système ou à un environnement SAN. Le nombre minimum de périphériques nécessaires pour une mise en miroir d'objets d'intégration SAP MaxDB, DB2 UDB ou Microsoft SQL Server est égal au nombre de périphériques utilisés pour la sauvegarde.

La charge de la mise en miroir d'objet est partagée par défaut. Data Protector exploite de façon optimale les périphériques disponibles en utilisant autant de périphériques que possible. Lorsque vous effectuez une opération de mise en miroir d'objet à partir de la ligne de commande, le partage de charge n'est pas disponible.

Copie d'un support

Vous pouvez copier des supports à des fins d'archivage ou de mise au coffre. Vous devez démarrer la copie de chaque support séparément, car un seul support peut être copié lors d'une session de copie de support.

Copie d'un support dans un périphérique autonome

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, développez **Périphériques**, cliquez avec le bouton droit sur le périphérique contenant le support à copier, puis cliquez sur **Copier**.
3. Sélectionnez le périphérique (lecteur et emplacement dans la bibliothèque) où se trouve le support cible, puis cliquez sur **Suivant**.
4. Sélectionnez le pool de supports auquel vous souhaitez ajouter la copie du support, puis cliquez sur **Suivant**.
5. Spécifiez la description et l'emplacement de la copie du support, puis cliquez sur **Suivant**.
6. Spécifiez des options supplémentaires pour la session : vous pouvez sélectionner l'option **Forcer opération**, spécifier la taille du support et sa protection.

   > **CONSEIL :**
   > Utilisez l'option **Forcer opération** si le support cible a d'autres formats reconnus par Data Protector (tar, OmniBack I, etc.) ou s'il s'agit de supports Data Protector sans protection.

7. Cliquez sur **Terminer** pour lancer la copie et quitter l'assistant.

Le message Informations sur la session affiche l'état de l'opération de copie des supports.

Copie d'un support dans un périphérique de bibliothèque

Procédure

1. Dans la liste de contexte, cliquez sur **Périphériques et supports**.
2. Dans la fenêtre de navigation, sous **Supports**, développez **Pools**, puis développez le pool de supports contenant le support à copier. Cliquez avec le bouton droit sur le support, puis cliquez sur **Copier** pour ouvrir l'assistant.
3. Sélectionnez un lecteur pour le support à copier et cliquez sur **Suivant**. Cette étape est ignorée si la bibliothèque ne contient qu'un seul lecteur.
4. Sélectionnez le périphérique (lecteur et emplacement dans la bibliothèque) où se trouve le support cible, puis cliquez sur **Suivant**.
5. Sélectionnez le pool de supports auquel vous souhaitez ajouter la copie du support, puis cliquez sur **Suivant**.
6. Spécifiez la description et l'emplacement de la copie du support, puis cliquez sur **Suivant**.
7. Spécifiez des options supplémentaires pour la session : vous pouvez sélectionner l'option **Forcer opération**, spécifier la taille du support et sa protection.

   > **CONSEIL :**
   > Utilisez l'option **Forcer opération** si le support cible a d'autres formats reconnus par Data Protector (tar, OmniBack I, etc.) ou s'il s'agit de supports Data Protector sans protection.

8. Cliquez sur **Terminer** pour lancer la copie et quitter l'assistant.

Le message Informations sur la session affiche l'état de l'opération de copie des supports.

Chapitre 13: Vérification d'objet

À propos de la vérification d'objet

La fonctionnalité de vérification d'objet Data Protector permet de vérifier des objets sauvegarde. Cette fonction élimine le besoin de vérification interactive d'un support de sauvegarde unique complet. Vous pouvez désormais vérifier des objets isolés ou multiples, sur des supports isolés ou multiples, de façon interactive, au cours de sessions planifiées ou lors de sessions post-opération.

Les objets vérifiés peuvent être des objets sauvegarde d'origine, des copies d'objets et des objets consolidés.

Vérification des données

Pendant une session de vérification d'objet, Data Protector vérifie les données des objets sauvegarde individuels de la même façon que lorsqu'il vérifie un support.

Restitution à l'hôte

Par défaut, l'hôte cible sur lequel le processus de vérification des données est effectué est l'hôte source de la sauvegarde d'origine. Ceci vient confirmer la capacité de Data Protector à restituer les données de sauvegarde de l'hôte de l'Agent de support vers cet hôte. Il est également possible d'indiquer un autre hôte cible, ou encore la vérification peut être effectuée sur l'hôte de l'Agent de support, de façon à éviter toute intervention du réseau.

Types de sessions de vérification d'objet

Vous pouvez démarrer une session de vérification d'objet de façon interactive ou définir un démarrage automatique de la session. Data Protector propose deux types de validation d'objet automatisée : la vérification d'objet post-sauvegarde et la vérification d'objet planifiée.

Vérification d'objet post-sauvegarde

La vérification d'objet post-sauvegarde est effectuée dès que les sessions de sauvegarde, de copie d'objet ou de consolidation d'objet se sont achevées, afin de vérifier les objets créés au cours de ces sessions. Les objets à vérifier sont spécifiés dans une spécification de vérification d'objet post-sauvegarde. Celle-ci spécifie les spécifications de sauvegarde et de copie et/ou de consolidation d'objet définissant les objets créés et fournit des critères permettant de les filtrer. Il est possible d'indiquer plusieurs spécifications de sauvegarde et de copie et/ou de consolidation d'objet dans une seule spécification de vérification d'objet post-sauvegarde.

Vérification d'objet planifiée

La vérification d'objet planifiée s'effectue aux heures définies dans le planificateur de Data Protector pour vérifier les versions des objets sauvegarde, copie ou consolidation créées au cours d'une période définie. Les

objets à vérifier et la période valide de création de versions des objets sont spécifiés dans une spécification de vérification d'objet planifiée. Celle-ci spécifie les spécifications de sauvegarde et de copie et/ou de consolidation d'objet définissant les objets créés et fournit des critères permettant de les filtrer. Il est possible d'indiquer plusieurs spécifications de sauvegarde et de copie et/ou de consolidation d'objet dans une seule spécification de vérification d'objet planifiée.

Comment vérifier des objets

Lancez tout d'abord une session interactive ou créez une spécification de vérification d'objet. Sélectionnez les objets sauvegarde à vérifier, les périphériques sources, les supports et l'hôte cible de la vérification.

Sélection des objets sauvegarde

Opération automatisée

Pour automatiser les spécifications de vérification d'objet, vous pouvez choisir les objets à vérifier en sélectionnant des spécifications de sauvegarde, de copie d'objet ou de consolidation, puis en les filtrant par protection, nombre de copies, bibliothèques disponibles ou période (planifiée seulement). Dans ce cas, il n’est pas possible de sélectionner des versions d'objet individuelles à des fins de vérification : Data Protector vérifie toutes les versions d'objet qui correspondent aux critères du filtre.

Opération interactive

Pour les sessions interactives, vous pouvez sélectionner des objets individuels parmi les supports, les sessions ou les listes de l'assistant de sélection d'objets dans l'IDB. Dans ce cas, il est possible de sélectionner des copies individuelles des versions des objets souhaitées en vue de leur validation.

Sélection d'un périphérique source

Par défaut, Data Protector effectue une sélection automatique du périphérique. Vous avez également la possibilité de forcer la sélection du périphérique d'origine ou d'en sélectionner un autre.

Sélection de l'hôte cible

Par défaut, Data Protector effectue le processus de vérification sur l'hôte source, à savoir celui sur lequel les objets source de la sauvegarde d'origine étaient situés, et vérifie les données de l'objet et leur restitution. Vous pouvez également indiquer un autre hôte distant, ou encore l'hôte de l'Agent de support, et ne vérifier que les données de l'objet. Notez qu'un un Agent de disque Data Protector doit être installé sur l'hôte cible sélectionné.

Planification

La planification des opérations de vérification planifiées s'effectue de la même manière qu'avec les sauvegardes, au moyen du planificateur Data Protector.

Pour plus d'informations sur la création et la modification de planifications dans Data Protector à l'aide du planificateur, voir *Planificateur, Page 110*.

> **IMPORTANT :**
> Avec Data Protector 10.00, les planificateur de base et avancé sont rendus obsolètes et remplacés par un nouveau planificateur Web. Vous pouvez configurer des sauvegardes sans surveillance en planifiant des sessions de sauvegarde à exécuter à des instants précis. Pendant la mise à niveau de Data Protector, toutes les planifications Data Protector existantes sont automatiquement migrées vers le nouveau planificateur.

Tâches de vérification d'objet standard

Voici les conditions préalables et les limites de la fonction de vérification d'objet :

Conditions préalables

- Vous devez installer un Agent de support sur chaque système qui servira d'hôte source au cours des sessions de vérification d'objet.
- Vous devez installer un Agent de disque sur chaque système qui servira d'hôte source au cours des sessions de vérification d'objet.
- Tous les Agents de disque intervenant dans le traitement de vérification d'objet doivent être de la version A.06.11 ou d'une version ultérieure.
- Les périphériques nécessaires doivent être configurés et les supports préparés.
- Pour démarrer une session de vérification d'objet, vous devez disposer des droits utilisateur appropriés sur les hôtes source et de destination : ce sont les droits utilisateur Démarrer la restauration et Restaurer à partir d'autres utilisateurs.
- Si l'hôte de destination fonctionne sous UNIX, vous devez disposer des autorisations Restaurer en tant que root.

Limites

- Les supports sources en cours de lecture ne sont pas disponibles pour la restauration.
- La vérification des objets intégration d'application consiste à vérifier que les données de l'objet sont remises à l'hôte cible et qu'elles présentent un format cohérent du point de vue de Data Protector. Aucune vérification spécifique à l'intégration n'est effectuée.
- La vérification d'objet n'est pas disponible pour les objets traités par une sauvegarde ZDB sur disque ou la partie disque de la sauvegarde ZDB sur disque + bande.

Vérification interactive des objets

Vous pouvez sélectionner des objets en vue d'une vérification interactive à partir du point de départ Supports, Objets ou Sessions, selon vos besoins. Vous ne pouvez pas enregistrer une spécification de vérification d'objets interactive ; vous pouvez uniquement lancer une session de vérification d'objets.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez **Vérification**, puis **Vérification d'objet**.
3. Développez la section **Interactive**.
4. Cliquez sur **Supports**, **Objets** ou **Sessions** pour ouvrir l'assistant.
   - Cliquez sur **Supports** pour afficher la liste des supports disponibles sur lesquels des objets ont été écrits.
   - Cliquez sur **Objets** pour afficher la liste des objets ayant été écrits sur les supports disponibles.
   - Cliquez sur **Sessions** pour afficher la liste des sessions durant lesquelles des objets ont été écrits sur les supports disponibles.
5. Sélectionnez les objets que vous souhaitez vérifier.

   > **REMARQUE :**
   > À partir de Data Protector 10.00 pour les sauvegardes VMware, les disques de la machine virtuelle sont considérés comme des objets qui s'exécutent en parallèle. Les objets disque de la machine virtuelle sont listés mais désactivés dans la liste **Supports** pour connaître les disques de la machine virtuelle qui sont sauvegardés sur le support. L'opération de copie ou de vérification est effectuée sur les objets de la machine virtuelle et tous ses objets disque associés sont pris en compte en interne.
   >
   > À partir de Data Protector 10.00 pour l'intégration VMware, l'option **Suivant** est activée uniquement après la sélection de l'objet de la machine virtuelle dans la liste **Supports**.

   Cliquez sur **Next**.
6. Sélectionnez le périphérique source sur lequel les objets doivent être lus. La sélection automatique de périphérique est activée par défaut.

   Vous pouvez également forcer la sélection de périphérique initiale ou y substituer un autre lecteur. Pour ce faire, cliquez avec le bouton droit de la souris sur **Périphérique d'origine**, puis sélectionnez **Changer périphérique**.

   Cliquez sur **Next**.
7. Sélectionnez l'hôte cible de l'opération de vérification d'objet. Cet hôte doit disposer d'un Agent de disque Data Protector avec le niveau de version requis installé.

   Par défaut, l'hôte source de la sauvegarde originale est sélectionné. Vous pouvez aussi sélectionner l'hôte Agent de support (sur lequel le périphérique source sélectionné est installé) ou un hôte arbitraire dans la cellule disposant d'un Agent de disque avec le niveau de version requis installé. Cliquez sur **Next**.
8. La liste des supports contenant les objets sélectionnés s'affiche. Lorsqu'un même objet réside sur plusieurs jeux de supports, vous pouvez modifier la priorité d'emplacement des supports pour influer sur leur sélection.

   Cliquez sur **Next**.
9. Un résumé des versions d'objets sélectionnées à des fins de vérification apparaît.

- Pour afficher des informations détaillées sur une version d'objet en particulier, sélectionnez-la dans la liste et cliquez sur **Propriétés**.

  S'il existe plusieurs copies d'une même version d'objet, Data Protector sélectionne par défaut la plus appropriée pour la vérification. Vous pouvez sélectionner manuellement la copie à vérifier dans les Propriétés.

  Cliquez sur **OK**.

- Pour supprimer une version d'objet de la liste, sélectionnez-la et cliquez sur **Supprimer**.

10. Cliquez sur **Terminer** pour quitter l'assistant et lancer la vérification.

Configuration de la vérification d'objet post-sauvegarde

La vérification d'objet post-sauvegarde est configurée pour se produire une fois que la session de sauvegarde, de copie d'objet ou de consolidation d'objet s'est achevée.

Les noms des spécifications de sauvegarde, de copie d'objet et/ou de consolidation concernées sont sélectionnés dans une spécification de vérification d'objet automatisée. Quand une session exécutée avec l'une de ces spécifications sélectionnées s'achève, Data Protector vérifie les objets produits au cours de la session en s'appuyant sur les critères fournis dans la spécification de vérification d'objet.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez **Vérification**, puis **Vérification d'objet**.
3. Développez **Automatique**, cliquez avec le bouton droit de la souris sur **Post-Sauvegarde** et sélectionnez **Ajouter** pour lancer l'assistant.
4. Sélectionnez les spécifications de sauvegarde que vous souhaitez faire suivre de la spécification de vérification d'objet. Cliquez sur **Next**.
5. Sélectionnez les spécifications de copie d'objets que vous souhaitez faire suivre de la spécification de vérification d'objet. Cliquez sur **Next**.
6. Sélectionnez les spécifications de consolidation que vous souhaitez faire suivre de la spécification de vérification d'objet. Cliquez sur **Next**.
7. Vous pouvez spécifier un filtre d'objets pour l'opération de vérification d'objet. Seuls les objets répondant aux critères spécifiés sont vérifiés. Cliquez sur **Next**.
8. Vous pouvez spécifier un filtre de bibliothèque pour l'opération de vérification d'objet. Seuls les objets résidant sur des supports figurant dans les bibliothèques spécifiées sont vérifiés. Cliquez sur **Next**.
9. Sélectionnez le périphérique source sur lequel les objets doivent être lus. Par défaut, Data Protector utilise une sélection automatique du périphérique.

   Vous avez également la possibilité de forcer la sélection du périphérique d'origine. Cela signifie que, si le périphérique n'est pas disponible, Data Protector attend qu'il le devienne. Vous pouvez également substituer un autre lecteur à celui d'origine. Pour ce faire, cliquez sur avec le bouton

droit de la souris sur **Périphérique d'origine**, puis sélectionnez **Changer périphérique**, par exemple à la suite du remplacement du périphérique d'origine par un neuf.

Cliquez sur **Next**.

10. Sélectionnez l'hôte cible de l'opération de vérification d'objet. Un Agent de disque Data Protector doit être installé sur cet hôte.

    Vous pouvez sélectionner :

    - l'hôte sur lequel l'objet sauvegarde d'origine a été produit (sélection par défaut). Cette opération vérifie également les composants de Data Protector sur le chemin d'accès réseau.
    - l'hôte de l'Agent de support, à savoir celui qui contient le périphérique source, sans intervention du réseau.
    - un autre hôte distant pour vérifier les composants de Data Protector sur le chemin d'accès réseau vers cet hôte.

    Cliquez sur **Next**.

11. Cliquez sur **Enregistrer sous...**, entrez un nom de spécification, puis cliquez sur **OK** pour enregistrer la spécification de vérification.

Configuration de la vérification d'objet planifiée

La vérification d'objet planifiée a lieu à l'heure définie par l'utilisateur. Les objets créés dans différentes sessions de sauvegarde, de copie d'objet ou de consolidation d'objet peuvent être vérifiés au cours d'une même session de vérification d'objet planifiée.

Procédure

1. Dans la liste de contexte, cliquez sur **Opérations sur les objets**.
2. Dans la fenêtre de navigation, développez **Vérification**, puis **Vérification d'objet**.
3. Développez **Automatique**, cliquez avec le bouton droit de la souris sur **Planifiée** et sélectionnez **Ajouter** pour lancer l'assistant.
4. Sélectionnez les spécifications de sauvegarde définissant les objets en sortie sur lesquels vous souhaitez planifier une vérification. Cliquez sur **Suivant**.
5. Sélectionnez les spécifications de copie d'objets définissant les objets en sortie sur lesquels vous souhaitez planifier une vérification. Cliquez sur **Suivant**.
6. Sélectionnez les spécifications de consolidation définissant les objets en sortie sur lesquels vous souhaitez planifier une vérification. Cliquez sur **Suivant**.
7. Vous pouvez spécifier un filtre d'objets pour l'opération de vérification d'objet.

   Vous êtes ainsi en mesure de filtrer les objets disponibles selon leur protection, leur nombre de copies ou leur date de création. Toutes les versions d'objet répondant aux critères de filtrage sont vérifiés.

   Cliquez sur **Suivant**.
8. Vous pouvez spécifier un filtre de bibliothèque pour l'opération de vérification d'objet. Seuls les

objets résidant sur des supports figurant dans les bibliothèques spécifiées sont vérifiés. Cliquez sur **Suivant**.

9. Sélectionnez le périphérique source sur lequel les objets doivent être lus. Par défaut, Data Protector utilise une sélection automatique du périphérique.

   Vous avez également la possibilité de forcer la sélection du périphérique d'origine. Cela signifie que, si le périphérique n'est pas disponible, Data Protector attend qu'il le devienne. Vous pouvez également substituer un autre lecteur à celui d'origine. Pour ce faire, cliquez sur avec le bouton droit de la souris sur **Périphérique d'origine**, puis sélectionnez **Changer périphérique**, par exemple à la suite du remplacement du périphérique d'origine par un neuf.

   Cliquez sur **Suivant**.

10. Sélectionnez l'hôte cible pour l'opération de vérification d'objet. Un Agent de disque Data Protector doit être installé sur cet hôte.

    Vous pouvez sélectionner :

    - l'hôte sur lequel l'objet sauvegarde d'origine a été produit (sélection par défaut). Cette opération vérifie également les composants de Data Protector sur le chemin d'accès réseau.
    - l'hôte de l'Agent de support, à savoir celui qui contient le périphérique source, sans intervention du réseau.
    - un autre hôte distant pour vérifier les composants de Data Protector sur le chemin d'accès réseau vers cet hôte.

    Cliquez sur **Suivant**.

11. Cliquez sur **Enregistrer et planifier...** Entrez un nom de spécification, puis cliquez sur **OK** pour enregistrer la spécification de vérification. Une fois la spécification enregistrée, l'assistant de planification s'ouvre. Suivez les étapes de l'assistant pour planifier la spécification.

    Pour plus d'informations sur la création et la modification de planifications dans Data Protector à l'aide du planificateur, consultez la rubrique *Planificateur, Page 110*.

Personnalisation de l'environnement de vérification d'objet

Vous pouvez personnaliser l'environnement de vérification d'objet en modifiant le niveau de message et l'état de session générés lorsqu'il n'y a aucun objet à vérifier lors d'une session de vérification. Pour cela, modifiez l'option globale `SessionStatusWhenNoObjectToVerify` .

Chapitre 14: Restaurer

À propos de la restauration

Le processus de restauration permet de recréer les données d'origine sur un disque à partir d'une copie de sauvegarde. Ce processus comprend la préparation et la restauration proprement dite des données, et éventuellement des actions consécutives à la restauration, visant à rendre les données disponibles pour l'utilisation.

Pour plus d'informations sur le concept de restauration, voir les documents *Guide conceptuel HPE Data Protector* et *Guide d'intégration HPE Data Protector*.

La spécification de ces fonctions et les options disponibles peuvent varier en fonction de la plate-forme utilisée.

Pour plus d'informations sur la procédure de restauration avec des intégrations avec des applications telles que Oracle, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server, Informix Server, IBM DB2 UDB ou Sybase, reportez-vous au document *Guide d'intégration HPE Data Protector*.

Procédure de restauration standard

La procédure de restauration standard se divise en plusieurs phases.

1. Sélection des données à restaurer.
2. Recherche des supports nécessaires.
3. Lancement de la session de restauration.

   Les autres paramètres sont prédéfinis en fonction du processus de sauvegarde suivi. Ils peuvent toutefois être modifiés.

Conditions préalables

Pour effectuer une restauration, vous devez disposer des droits utilisateur appropriés. Ces droits sont définis en fonction du groupe d'utilisateurs.

Sélection des données à restaurer

Vous pouvez parcourir les données à restaurer de deux manières possibles : soit à partir de la liste des objets sauvegardés, soit depuis la liste des sessions. La différence réside dans la portée des répertoires et fichiers présentés pour la restauration :

- **Restaurer des objets** avec une liste d'objets sauvegardés classés par systèmes clients dans la cellule et par différents types de données (par exemple système de fichiers, image disque, base de données interne et ainsi de suite). Vous pouvez parcourir tous les répertoires, fichiers et versions, qui ont été sauvegardés et sont toujours disponibles pour restauration.
- **Restaurer des sessions** avec une liste de sessions de système de fichiers avec tous les objets sauvegardés dans ces sessions. Vous pouvez choisir d'afficher uniquement les sessions de l'année

dernière, du mois dernier ou de la semaine dernière. Vous pouvez parcourir tous les objets qui ont été sauvegardés dans cette session (comme tous les lecteurs de tous les clients nommés dans la spécification de sauvegarde), et toutes les versions de cette chaîne de restauration. Par défaut, la chaîne de restauration entière de répertoires ou fichiers sélectionnés est restaurée, mais vous pouvez également restaurer les données d'une seule session.

Conditions préalables

Afin de parcourir les objets et sélectionner des répertoires ou des fichiers spécifiques, les sauvegardes correspondantes doivent avoir été effectuées en utilisant un niveau de journalisation de niveau répertoire, nom de fichier ou journaliser tout.

Sélection des données de la liste d'objets sauvegardés

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié (par exemple **système de fichiers**).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié (point de montage pour des systèmes UNIX, lecteur pour des systèmes Windows).
4. Dans la page de propriétés Source, développez l'objet, puis sélectionnez les répertoires ou fichiers à restaurer.

   Par défaut, lorsque vous sélectionnez un répertoire complet, seuls les répertoires et/ou fichiers de la dernière session de sauvegarde sont sélectionnés pour la restauration. Les répertoires et fichiers de l'arborescence qui n'ont pas été sauvegardés lors de la même session sont grisés. Pour restaurer les données à partir d'une autre session de sauvegarde, cliquez avec le bouton droit sur le répertoire sélectionné et choisissez **Restaurer version**. Dans la liste déroulante Version de sauvegarde, sélectionnez la version à restaurer.

> **CONSEIL :**
> Si vous répétez les étapes ci-dessus et sélectionnez des données sous plus d'un objet (point de montage ou lecteur), vous pouvez effectuer une restauration parallèle.

Sélection des données de la liste de sessions de sauvegarde

Limites

- Vous ne pouvez pas restaurer les intégrations de base de données en ligne à partir d'une session de sauvegarde spécifique.
- Vous ne pouvez pas utiliser le mode "Sessions de restauration" pour effectuer une restauration à partir d'une session de copie.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, développez **Restaurer sessions** pour afficher les clients puis les objets sauvegardés sur un client particulier. Cliquez sur un objet pour ouvrir les pages de propriétés de l'objet.
3. Dans la page **Source**, sélectionnez les répertoires ou les fichiers à restaurer.

   Par défaut, la chaîne de restauration entière est restaurée (**Afficher la chaîne complète** est sélectionné). Pour restaurer uniquement les données de cette session, sélectionnez **Afficher cette session uniquement**.
4. Spécifiez la destination de la restauration et définissez les options de restauration.
5. Cliquez sur **Restaurer** pour démarrer la session de restauration.

> **CONSEIL :**
> Pour effectuer une restauration parallèle, répétez les étapes 2 à 4 pour les objets supplémentaires avant de lancer la restauration.

Sélection d'une version de sauvegarde spécifique

Après avoir sélectionné les données à restaurer, vous pouvez sélectionner la version de sauvegarde.

Sélectionner séparément la version de sauvegarde de chaque fichier ou répertoire

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié (par exemple système de fichiers).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié.
4. Dans la page de propriétés Source, sélectionnez l'objet à restaurer. Par défaut, la dernière version de sauvegarde est sélectionnée pour la restauration.
5. Cliquez avec le bouton droit de la souris sur l'objet, puis sélectionnez **Restaurer version**.
6. Dans la liste déroulante Version de sauvegarde, sélectionnez la version à restaurer. Cliquez sur "**...**pour obtenir plus d'informations sur les versions de sauvegarde. Le bouton "**...**" est disponible si la sauvegarde a été effectuée avec un niveau de journalisation permettant de journaliser les attributs.
7. Cliquez sur **OK**.

Une fois que vous avez sélectionné une version pour la restauration, seuls les fichiers et répertoires de cette version peuvent être sélectionnés dans la page de propriétés Source. Les autres fichiers et répertoires apparaissent en grisé et ne seront pas restaurés.

Sélectionner la version de sauvegarde de plusieurs fichiers ou répertoires en même temps

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié (par exemple **système de fichiers**).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié.
4. Dans la page de propriétés Source, sélectionnez plusieurs objets à restaurer. Par défaut, la dernière version de sauvegarde est sélectionnée pour la restauration.
5. Cliquez sur l'onglet **Résumé de restauration**, puis sélectionnez tous les objets. Cliquez ensuite avec le bouton droit sur la sélection et cliquez sur **Sélectionner version par date**.
6. Cliquez sur l'option **Sélectionner version par date et heure**, puis sélectionnez le jour dans le menu contextuel.
7. Pour saisir l'heure, cliquez sur une valeur de la liste déroulante **Sélectionner version par date et heure**.
8. Sous **Différences dans l'heure de sauvegarde**, apportez les modifications nécessaires s'il n'existe aucune version de sauvegarde correspondant à votre sélection de date et d'heure pour les objets sélectionnés.
9. Sous **Si date et heure sélectionnées ne correspondent pas aux critères**, apportez les modifications nécessaires s'il n'existe aucune version de sauvegarde correspondant à votre sélection de date et d'heure ou aux modifications apportées sous **Différences dans l'heure de sauvegarde** pour les objets sélectionnés.
10. Cliquez sur **OK**.

Une fois les critères de restauration spécifiés, les versions de sauvegarde correspondant à votre sélection s'affichent dans la page de propriétés Source en regard de chaque objet à restaurer.

Gestion des conflits de fichiers

Vous pouvez choisir la façon dont le système doit résoudre les conflits entre la version du fichier se trouvant sur le disque et celle provenant de la sauvegarde.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié (par exemple **système de fichiers**).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié.
4. Dans la page de propriétés Source, sélectionnez le disque, les répertoires ou les fichiers à

restaurer.

5. Cliquez sur l'onglet **Destination** , puis sous Gestion de conflit de fichiers, sélectionnez l'une des options disponibles :
   - **Garder le plus récent**
   - **Ne pas écraser**
   - **Ecraser**

Sélection d'un périphérique pour la restauration

Par défaut, Data Protector restaure des données sélectionnées sur les périphériques utilisés pour la sauvegarde. Vous avez toutefois la possibilité d'utiliser d'autres périphériques pour la restauration.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié (par exemple **système de fichiers**).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié.
4. Dans la page de propriétés Source, développez l'objet, puis sélectionnez les éléments à restaurer.
5. Cliquez sur l'onglet **Périphériques** pour ouvrir la page de propriétés Périphériques.

   Les périphériques utilisés au cours de la sauvegarde y apparaissent.

   Pour restaurer les données sur un autre périphérique, sélectionnez le périphérique d'origine, puis cliquez sur **Modifier**. Effectuez votre sélection dans la boîte de dialogue Sélectionner nouveau périphérique, puis cliquez sur **OK**. Le nom du nouveau périphérique apparaît sous Etat du périphérique. Ce nouveau périphérique ne servira que pour cette session.

   Pour obtenir des informations sur le périphérique, cliquez dessus avec le bouton droit, puis cliquez sur **Infos**.

   Indiquez l'opération que Data Protector doit effectuer si les périphériques sélectionnés ne sont pas disponibles pour la restauration (s'ils sont, par exemple, désactivés ou en cours d'utilisation). Sélectionnez **Sélection auto du périphérique** ou **Sélection du périphérique d'origine**.

Recherche des supports nécessaires à la restauration

Une fois les données à restaurer sélectionnées, vous devez obtenir la liste des supports contenant les données. Cette étape est primordiale si vous utilisez des périphériques autonomes ou si vous conservez des supports en dehors de la bibliothèque.

Si une version d'objet que vous voulez restaurer existe sur plusieurs jeux de supports, vous pouvez influer sur la sélection du jeu de supports qui sera utilisé pour la restauration en spécifiant la priorité d'emplacement des supports, ou sélectionner manuellement le support à utiliser.

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

> **REMARQUE :**
> Les copies obtenues à l'aide de la fonctionnalité de copie de supports n'apparaissent pas comme des supports requis. Une copie de support n'est utilisée que si le support d'origine (celui qui a servi de source pour la copie) n'est pas disponible ou pas utilisable.

Limites

- Avec certaines intégrations, il n'est pas possible de définir la priorité pour l'emplacement des supports dans le contexte de restauration. L'interface n'affiche pas l'onglet Supports pour ces intégrations.
- Vous ne pouvez pas sélectionner manuellement le jeu de supports lorsque vous restaurez des objets d'intégration.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié (par exemple **système de fichiers**).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié.
4. Dans la page de propriétés Source, développez l'objet, puis sélectionnez les éléments à restaurer.
5. Cliquez sur l'onglet **Support**s pour ouvrir la page de propriétés du support. Cette page contient les supports nécessaires. Pour obtenir des informations sur un support, cliquez dessus avec le bouton droit de la souris, puis sélectionnez **Infos**.

   Si une version d'objet que vous voulez restaurer existe sur plusieurs jeux de supports, le système affiche tous les supports qui contiennent cette version. La sélection du jeu de supports dépend de l'algorithme interne de Data Protector et du paramètre de priorité défini pour l'emplacement des supports.

   - Pour modifier la priorité d'emplacement des supports, sélectionnez un emplacement, puis cliquez sur **Changer la priorité**. Sélectionnez une priorité différente pour l'emplacement, puis cliquez sur **OK**.
   - Pour sélectionner manuellement le jeu de supports depuis lequel doit s'effectuer la restauration, cliquez sur l'onglet **Copies**. Dans la page de propriétés Copies, sélectionnez la version d'objet de votre choix, puis cliquez sur **Propriétés**. Choisissez l'option **Sélectionner la copie source manuellement**, sélectionnez la copie de votre choix dans la liste déroulante, puis cliquez sur **OK**.
6. Le cas échéant, insérez les supports dans le périphérique.

> **CONSEIL :**
> Vous pouvez également afficher les supports nécessaires pour la restauration, notamment ceux contenant des copies des objets sélectionnés, en cliquant sur **Support requis** dans la

boîte de dialogue Démarrer session de restauration. Cette boîte de dialogue s'affiche lorsque vous démarrez la restauration.

Test et démarrage d'une restauration

Conditions préalables

- Assurez-vous que les supports nécessaires sont disponibles ou qu'ils sont chargés dans le périphérique.

Limites

- Il n'y a pas de test disponible pour la restauration de base de données interne Data Protector et les sessions d'intégration d'application Data Protector.

Procédure

1. Sélectionnez les éléments à restaurer, puis spécifiez les options dans les pages de propriétés de la restauration, sans oublier de sélectionner le périphérique à utiliser.
2. Identifiez les supports à utiliser pour la restauration.
3. Dans le menu **Actions**, cliquez sur **Tester la restauration** si vous souhaitez exécuter un test ou sur **Démarrer la restauration** pour lancer effectivement le processus de restauration. Vous pouvez également cliquer sur le bouton **Tester** ou **Restaurer** dans une page **Propriétés**.
4. Dans l'assistant de démarrage de session, vérifiez votre sélection et spécifiez les options **Niveau de rapport**, **Charge réseau** et **Activer la reprise des restaurations**.

Le moniteur de restauration affiche la progression de l'opération.

Abandon d'une restauration

L'abandon d'une session de restauration arrête le processus de restauration. Les données traitées avant que la session n'ait été abandonnée sont toutefois restaurées à l'emplacement spécifié.

Procédure

1. Pour abandonner une session de restauration, cliquez sur **Abandonner** dans le menu **Actions**.

CONSEIL :
Vous pouvez abandonner des sessions de restauration à partir du moniteur Data Protector.

Options d'emplacement de restauration

Par défaut, Data Protector restaure les données vers le client et le répertoire à partir desquels elles ont été sauvegardées. Vous pouvez modifier ces paramètres par défaut dans la page de propriétés Destination en spécifiant vers quel emplacement les données doivent être restaurées :

- avec les droits utilisateur appropriés, vous pouvez effectuer la restauration vers un autre système client
- Vous pouvez restaurer les données vers un autre répertoire.

Vous pouvez spécifier l'emplacement général pour la restauration objet par objet.

Data Protector propose également l'option **Restaurer sous/dans** qui permet de spécifier un autre emplacement pour les différents fichiers et répertoires du même objet sauvegarde.

Sélection d'un emplacement de restauration

Après avoir sélectionné les données à restaurer, vous pouvez définir l'emplacement vers lequel doit s'effectuer la restauration. Vous pouvez restaurer les données sur un autre système client et modifier le chemin d'accès au répertoire. Cette fonction permet de restaurer uniquement des objets complets.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié.
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié.
4. Dans la page de propriétés Source, sélectionnez l'objet à restaurer.
5. Cliquez sur l'onglet **Destination**, puis, dans la liste déroulante **Client cible**, sélectionnez le système client à restaurer sur le nouveau client. Par défaut, Data Protector utilise la structure de répertoires d'origine pour la restauration : si les données ont été sauvegardées à partir du répertoire `C:\temp` du système `A`, les données sont restaurées dans le répertoire `C:\temp` du système `B`.
6. Pour modifier le chemin d'accès au répertoire pour la restauration, sélectionnez l'option **Restaurer vers nouvel emplacement** et saisissez ou recherchez un nouveau répertoire d'ancrage. Le chemin d'accès au répertoire utilisé pour la sauvegarde est ajouté à celui du nouveau répertoire d'ancrage : si les données ont été sauvegardées à partir du répertoire `C:\sound\songs` et que vous spécifiez comme nouveau chemin d'accès `\users\bing`, les données sont restaurées dans le répertoire `C:\users\bing\sound\songs`.

Spécification d'un emplacement de restauration pour différents fichiers et répertoires

Vous pouvez indiquer un chemin de restauration spécifique pour tout répertoire ou fichier de chaque objet. L'emplacement particulier spécifié pour l'option **Restaurer sous/dans** remplace l'emplacement défini dans la page de propriétés Destination.

Cette option est disponible pour le noeud d'arborescence initialement sélectionné (répertoire) et pour tous les noeuds qui ne sont pas hiérarchiquement dépendants d'un noeud déjà sélectionné. Un noeud d'arborescence sélectionné est indiqué par une coche bleue et un noeud dépendant par une coche noire.

Restaurer dans

Restaurer dans ajoute le chemin d'accès provenant de la sauvegarde au nouvel emplacement sélectionné. Le nouvel emplacement doit correspondre à un répertoire existant.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié.
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié.
4. Dans la page de propriétés Source, sélectionnez l'objet à restaurer.
5. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire, puis sélectionnez **Restaurer sous/dans**.
6. Sous l'onglet Destination, dans la liste déroulante Restaurer, sélectionnez **Dans**.
7. Sur les systèmes Windows, vous pouvez sélectionner un autre lecteur vers lequel restaurer les données en saisissant son nom dans la zone de texte Lecteur. Si vous souhaitez effectuer la restauration sur un autre client, cliquez sur **Parcourir**.
8. Dans la zone de texte Emplacement, entrez un nouveau chemin d'accès pour le fichier ou le répertoire. Le chemin d'accès d'origine est ajouté au nouveau : si le fichier `colors.mp3` a été sauvegardé à partir du répertoire `C:\sound\songs` et que vous spécifiez comme nouveau chemin d'accès `\users\bing` , le fichier est restauré dans le répertoire `C:\users\bing\sound\songs`.
9. Cliquez sur **OK**.

Restaurer sous

Restaurer sous permet de remplacer le chemin d'accès utilisé pour la sauvegarde par celui du nouvel emplacement sélectionné. Le chemin de destination peut être un nouveau répertoire ou un répertoire existant. Vous pouvez renommer les fichiers et les répertoires lors de la restauration.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié.
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié.
4. Dans la page de propriétés Source, sélectionnez l'objet à restaurer.
5. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire, puis sélectionnez **Restaurer sous/dans**.
6. Sous l'onglet Destination, dans la liste déroulante Restaurer, sélectionnez **Sous**.
7. Sur les systèmes Windows, vous pouvez sélectionner un autre lecteur vers lequel restaurer les données en saisissant son nom dans la zone de texte Lecteur. Si vous souhaitez effectuer la restauration sur un autre client, cliquez sur **Parcourir**.
8. Dans la zone de texte Emplacement, entrez un nouveau chemin d'accès pour le fichier ou le

répertoire. Par exemple, si le fichier `colors.mp3` a été sauvegardé à partir du répertoire `C:\sound\songs` et que vous spécifiez comme nouveau chemin d'accès `\users\bing\colors.mp` , le fichier est restauré dans le répertoire `C:\users\bing`.

> **ATTENTION :**
> Prenez en compte le risque inhérent à la suppression de données avec l'option **Ecraser** activée quand :
>
> - vous spécifiez des éléments à restaurer sous un nom existant,
> - vous saisissez un chemin d'accès existant sans spécifier le nom du fichier/répertoire.
>
> Par exemple, lorsque vous entrez le nouveau chemin d'accès `\users\bing` dans la zone de texte Emplacement pour restaurer le fichier `colors.mp` mais n'avez pas entré le nom du fichier, `colors.mp` est alors restauré sous `bing`. L'ancien répertoire `bing` est alors supprimé et remplacé par le fichier restauré.

9. Cliquez sur **OK**.

A propos de la reprise de sessions ayant échoué

Les sessions de sauvegarde et de restauration ayant échoué pour l'une des raisons suivantes peuvent être redémarrées à l'aide de la fonctionnalité de reprise de sessions de Data Protector :

- Problème de connectivité réseau
- Problème fatal de l'Agent de disque
- Problème fatal de l'Agent de support
- Problème fatal du gestionnaire de session
- Problème fatal de support (par exemple bande déchirée)
- Commande Abandonner invoquée depuis l'interface graphique

Toutefois, vous devez tout d'abord résoudre le problème.

Lorsque vous reprenez une session ayant échoué, Data Protector poursuit la sauvegarde ou la restauration à partir de là où la session échouée s'est arrêtée. La session reprise hérite de toutes les options de la session d'origine.

La reprise n'est pas possible sur tous les types de sessions. Data Protector peut exécuter la reprise de :

- Sessions de sauvegarde du système de fichier
- Sessions de restauration du système de fichier
- Sessions de sauvegarde de l'intégration de Data Protector avec Oracle Server
- Sessions de restauration de l'intégration de Data Protector avec Oracle Server

Sessions de sauvegarde du système de fichier

Le fonctionnalité de reprise de session pour les sessions de sauvegarde du système de fichiers est basée sur les informations du fichier de point de contrôle écrites dans la base de données interne. Lorsqu'une session de sauvegarde échoue, le dernier fichier sauvegardé est marqué comme point de contrôle dans la base de données interne. Ainsi, la session de sauvegarde peut continuer depuis le

point d'échec lorsque la session reprend. Le fichier au point d'échec est sauvegardé dès le début, tandis que les données restantes sont ajoutées à la session de sauvegarde d'origine en tant que sauvegarde incrémentale. La session reprise hérite automatiquement de toutes les options de la session d'origine.

Si le fichier marqué comme point de contrôle est supprimé du système de fichiers, la fonctionnalité de reprise peut toujours déterminer les données qui n'ont pas encore été sauvegardées. Une session de sauvegarde ayant échoué peut être reprise plusieurs fois jusqu'à sa complétion.

Dans l'interface utilisateur, la session peut être reprise avec le menu contextuel de la session ayant échoué. Dans l'interface de lignes de commande, la session peut être restaurée à l'aide de l'option `omnib -resume`.

Limites

- La reprise n'est pas prise en charge pour la récupération après sinistre.
- La reprise n'est pas prise en charge pour les sessions contenant des objets de format de données de support NDMP.
- Les objets sauvegardés avec les systèmes client de sauvegarde ne sont pas synthétisables : Solaris 9, SCO OpenServer et OpenVMS.

Sessions de restauration du système de fichier

La fonctionnalité de reprise pour les sessions de restauration du système de fichiers est fondée sur les fichiers de point de contrôle créés lors d'une session de restauration et contient des informations sur les options de restauration utilisées au cours de la session, ainsi que sur les fichiers qui ont été restaurés correctement. Dès qu'un nouveau fichier est restauré, le fichier de point de contrôle correspondant est actualisé.

Par défaut, les fichiers de point de contrôle sont créés sur le Gestionnaire de cellule et le client de destination (le fichier de point de contrôle contenant des informations sur les options de restauration n'est créé que sur le Gestionnaire de cellule).

Sur le Gestionnaire de cellule, les fichiers de point de contrôle sont créés dans :

Systèmes Windows : `\config\server\sessions\checkpoint`

Systèmes UNIX : `/var/opt/omni/server/sessions/checkpoint`

Sur les clients, les fichiers de vérification sont créés dans le répertoire de fichiers provisoires par défaut Data Protector, dans le sous-répertoire `Checkpoint`.

Fonctionnement

Lorsque vous reprenez une session de restauration ayant échoué, Data Protector lit les informations des fichiers de point de contrôle et poursuit la restauration à partir du point où la session de restauration ayant échoué s'est interrompue. En fait, quand vous reprenez une session de restauration, ses fichiers de point de contrôle sont déplacés dans le répertoire des fichiers de point de contrôle de la session de restauration de reprise, où ils continuent à être actualisés. Par conséquent, une session de restauration ayant échoué ne peut être reprise qu'une fois. Si vous tentez de reprendre la session échouée une deuxième fois, l'opération échoue car les fichiers de point de contrôle ne sont plus présents.

Points à prendre en considération

- Dans les environnements de cluster, assurez-vous que les fichiers de point de contrôle sont créés sur un disque partagé, de telles sorte que les deux nœuds de cluster puissent y accéder. Pour modifier l'emplacement des fichiers de vérification, utilisez l'option omnirc `OB2CHECKPOINTDIR`. L'option doit être définie sur les deux nœuds de cluster et doit pointer vers le même répertoire.
- Vous pouvez désactiver la création de fichiers de point de contrôle en désélectionnant l'option **Activer la reprise des restaurations** avant de démarrer une session de restauration (l'option se situe dans la boîte de dialogue Démarrer session de restauration, à la fin de l'assistant de restauration). Toutefois, en cas d'échec de la session de restauration, vous n'êtes pas en mesure de la relancer, car les fichiers de point de contrôle sont absents. Les sessions qui se sont achevées correctement ne peuvent pas être relancées non plus, puisque Data Protector supprime les fichiers de point de contrôle lorsqu'elles prennent fin.
- Une session de restauration reprise ne s'achevant pas correctement peut également faire l'objet d'une reprise. Ceci est dû au fait qu'une session de restauration reprise hérite des fichiers de point de contrôle de la session d'origine. Elle hérite ainsi des options de restauration utilisées dans la session d'origine, dont l'option **Activer la reprise des restaurations**.
- Lorsqu'une session de restauration est supprimée de la base de données interne (par défaut les sessions sont supprimées au bout de 30 jours), ses fichiers de point de contrôle sont également purgés. Les fichiers de vérification sont également purgés lorsque vous lancez l'IDB à l'aide de la commande `omnidbinit`.
- Si l'option **No overwrite** a été utilisée pour restaurer un ou plusieurs objets dans un session en échec, l'option `omnirc OB2NOOVERWRITE_TRAVERSEDIROBJ` doit être définié à 1 avant que vous ne fermiez cette session.

Limites

- Si une session de restauration échoue parce que le client de destination est tombé en panne, la fonctionnalité de reprise de session risque de ne pas fonctionner correctement. Tout dépend du fait que les fichiers de point de contrôle aient été ou non vidés de la mémoire vers le disque au moment de la panne du client.
- Si une session de restauration échoue au cours de la restauration de fichiers de lien réel, il se peut que la fonctionnalité de reprise de restauration ne soit pas en mesure de restaurer les fichiers en lien réel restants. Cela est dû au fait que, durant la sauvegarde, Data Protector ne sauvegarde un fichier en lien réel qu'une seule fois. Pour les autres fichiers faisant l'objet d'une liaison réelle, seule la référence au fichier est sauvegardée. En conséquence, les restaurations de fichiers à liens réels sont interconnectées et ceux-ci doivent donc tous être restaurés en même temps. Notez que le problème ne survient pas si la session de restauration échoue avant que la restauration des fichiers à liaison réelle n'ait commencé ou ne se soit terminée.
- Supposons que vous souhaitiez restaurer un arbre qui a été sauvegardé dans les sessions suivantes Full, Incr. et Incr. Si la session de restauration échoue car l'objet sauvegarde arborescence créé dans l'une des sessions de sauvegarde n'est pas disponible (par exemple, les supports utilisés au cours de la dernière session de sauvegarde Incr sont altérés), vous devez fournir la copie de cet objet sauvegarde. Si une telle copie d'objet n'existe pas, vous ne pouvez pas reprendre la session de restauration ayant échoué, même si une sauvegarde complète synthétique de l'objet sauvegarde manquant existe.

Sessions de sauvegarde et de restauration de l'intégration de Data Protector avec Oracle Server

La fonctionnalité Redémarrer la session pour les sessions de sauvegarde et de restauration Data Protector Oracle Server integration est décrite dans le *Guide d'intégration HPE Data Protector*.

Reprise de sessions ayant échoué

Les sessions de sauvegarde et de restauration ayant échoué (par exemple, en raison de problèmes de connectivité réseau) peuvent être redémarrées à l'aide de la fonctionnalité de reprise de sessions de Data Protector. Lorsque vous redémarrez une session ayant échoué, Data Protector poursuit la sauvegarde ou la restauration, en commençant où la session ayant échoué s'est arrêtée.

Conditions préalables

- Vous devez être membre du groupe d'utilisateurs Admin Data Protector ou disposer des droits utilisateur Moniteur Data Protector.

Procédure

1. Si vous utilisez un Gestionnaire de cellule ordinaire, cliquez sur **Base de données interne** dans la liste de contexte.

   Si vous utilisez un Manager-of-Managers, choisissez **Clients** dans la liste de contexte, puis développez **Clients d'entreprise**. Sélectionnez un Gestionnaire de cellule rencontrant un problème de session. Dans le menu Outils, sélectionnez **Administration base de données** pour ouvrir une nouvelle fenêtre d'interface utilisateur Data Protector dans laquelle apparaît le contexte de la base de données interne.
2. Dans la fenêtre de navigation, développez **Base de données interne**, puis cliquez sur **Sessions**.

   Une liste de sessions s'affiche dans la zone de résultats. L'état de chaque session est indiqué dans la colonne Etat.
3. Cliquez avec le bouton droit sur une session ayant échoué et sélectionnez **Reprendre la session**.

Tâches de restauration avancées

Il est possible de contrôler une restauration de plusieurs façons. Data Protector propose un ensemble de tâches de restauration avancées pour les systèmes Windows et UNIX.

Conditions préalables

- Pour effectuer une restauration, vous devez disposer des droits utilisateur appropriés. Ces droits sont définis en fonction du groupe d'utilisateurs.
- Avant de poursuivre, vous devez prendre connaissance de la procédure de restauration standard.

Tâches de restauration avancées

Il s'agit de la spécification d'options rarement utilisées ou d'une action qui ne suit pas la procédure de restauration standard. Pour restaurer les données, vous devrez toutefois suivre la plupart des étapes requises pour une restauration standard.

La façon dont vous suivez la procédure de restauration standard dépend de la tâche avancée que vous souhaitez effectuer. Par exemple, vous pouvez restaurer vos données sans navigation. Vous devez alors spécifier les données d'une autre façon. Pour les autres étapes, vous pouvez suivre la procédure de restauration standard.

- Fichiers ignorés lors de la restauration
- Sélection de certains fichiers (correspondant à une recherche) à restaurer
- Sélection des fichiers ouverts pour la restauration
- Refus de l'accès aux fichiers lors de la restauration
- Recherche d'un fichier à restaurer
- Sélection d'un disque partagé Windows pour la restauration
- Restauration d'objets en parallèle
- Restauration d'une image disque
- Restauration depuis des supports provenant d'un coffre
- Restauration d'un serveur Web
- Restauration sans exploration

Fichiers ignorés lors de la restauration

Data Protector permet d'ignorer des fichiers qui ont été sauvegardés mais que vous ne souhaitez pas restaurer. Grâce aux caractères génériques, vous pouvez ignorer les fichiers correspondant à un modèle de recherche spécifique.

> **REMARQUE :**
> Cette fonctionnalité n'est pas prise en charge par l'intégration de Data Protector avec le serveur.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, développez le type de données approprié (par exemple, **système de fichiers**).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié (point de montage pour des systèmes UNIX, lecteur pour des systèmes Windows).
4. Dans la page de propriétés Source, sélectionnez le répertoire à restaurer.
5. Cliquez avec le bouton droit de la souris sur le répertoire, puis cliquez sur **Propriétés**.
6. Cliquez sur l'onglet **Ignorer**.

7. Dans la zone de texte, saisissez le nom de fichier ou un critère permettant de trouver les fichiers à ignorer (par exemple : `*.mp3`), puis cliquez sur **Ajouter**. Dans cet exemple, aucun fichier `mp3` ne sera restauré. Pour ajouter un critère, renouvelez cette étape.
8. Cliquez sur **OK**.

Sélection de certains fichiers (correspondant à une recherche) à restaurer

Data Protector permet de restaurer uniquement les fichiers de la sauvegarde qui correspondent à un modèle de recherche spécifique. Grâce aux caractères génériques, vous pouvez indiquer le modèle à utiliser.

> **REMARQUE :**
> Cette fonctionnalité n'est pas prise en charge par l'intégration de Data Protector avec le serveur NDMP.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, développez le type de données approprié (par exemple, système de fichiers).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié (point de montage pour des systèmes UNIX, lecteur pour des systèmes Windows).
4. Dans la page de propriétés Source, sélectionnez le répertoire à restaurer.
5. Cliquez avec le bouton droit de la souris sur le répertoire, puis cliquez sur **Propriétés**.
6. Cliquez sur l'onglet **Restaurer uniquement**.
7. Dans la zone de texte, saisissez les nom des fichiers ou un critère permettant de trouver les fichiers à restaurer, par exemple, `*.mp3`, puis cliquez sur **Ajouter**. Seuls les fichiers `mp3` seront restaurés. Pour ajouter un critère, renouvelez cette étape.
8. Cliquez sur **OK**.

Sélection des fichiers ouverts pour la restauration

Par défaut, Data Protector ne restaure pas les fichiers en cours d'utilisation par d'autres applications (fichiers ouverts). Pour restaurer également ces fichiers, procédez comme suit.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, développez le type de données approprié (par exemple, **système de fichiers**).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié (point de montage pour des systèmes UNIX, lecteur pour des systèmes Windows).

4. Dans la page de propriétés Source, développez l'objet, puis sélectionnez les éléments à restaurer.
5. Cliquez sur l'onglet **Options**, puis activez l'option **Déplacer fichiers occupés**.

Refus de l'accès aux fichiers lors de la restauration

Par défaut, Data Protector ne verrouille pas les fichiers lors de la restauration. Vous pouvez cependant modifier ce comportement par défaut.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, développez le type de données approprié (par exemple, **système de fichiers**).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié (point de montage pour des systèmes UNIX, lecteur pour des systèmes Windows).
4. Dans la page de propriétés Source, développez l'objet, puis sélectionnez les éléments à restaurer.
5. Cliquez sur l'onglet **Options**, puis activez l'option **Verrouiller les fichiers pendant la restauration**.

Recherche d'un fichier à restaurer

Si vous ne connaissez pas le chemin d'accès complet d'un fichier à restaurer, vous pouvez rechercher ce fichier dans l'IDB (base de données interne), à condition que le niveau de journalisation au moment de la sauvegarde ait été défini sur Journaliser fichiers ou Journaliser tout. Vous pouvez rechercher des fichiers et des répertoires à l'aide de la tâche **Restaurer par requête** si vous connaissez au moins une partie du nom des fichiers.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Cliquez sur l'onglet de navigation **Tâches** au bas de la fenêtre de navigation. Les tâches de restauration prédéfinies sont fournies dans la fenêtre de navigation.
3. Cliquez sur Restaurer par requêtepour ouvrir l'assistant.
4. Spécifiez une partie du nom de fichier à l'aide de caractères génériques.

   Par exemple, entrez `*.exe` pour rechercher tous les fichiers sauvegardés avec cette extension.

   Lorsque vous spécifiez des caractères non ASCII, vérifiez que le codage actuel de l'interface graphique de Data Protector est le même que celui utilisé lors de la création des fichiers. Sinon, Data Protector ne trouvera pas les fichiers.

   Dans l'environnement d'un gestionnaire de cellule UNIX, le caractère générique `?` ne produira pas les résultats escomptés si vous tentez de rechercher un caractère multi-octets associé. Vous devez spécifier plusieurs caractères génériques `?`.. Par exemple, s'il faut `3` octets pour représenter le caractère multi-octets avec le codage actuel, ajoutez `???` à votre chaîne.

Si les répertoires sont disponibles, comparez uniquement le nom de base avec les modèles. Si les répertoires sont disponibles, comparez le nom complet du chemin d'accès avec les modèles.

5. Vous pouvez spécifier d'autres paramètres (facultatif). Cliquez sur **Next**.
6. Vous pouvez spécifier la période de sauvegarde et de modification des fichiers (facultatif). Cliquez sur **Next**.

   Data Protector fournira la liste de tous les fichiers et répertoires correspondant aux critères définis.
7. Dans la liste des fichiers correspondant aux critères de sélection, choisissez les fichiers à restaurer. Pour spécifier d'autres options, cliquez sur l'onglet approprié. Pour configurer les options **Niveau de rapport**, **Charge réseau** et **Activer la reprise des restaurations**, cliquez sur **Suivant**. Pour lancer la restauration, cliquez sur **Terminer**.

Sélection d'un disque partagé Windows pour la restauration

Data Protector permet de restaurer des données vers un disque partagé, même si elles n'ont pas été initialement sauvegardées à partir du disque partagé.

Vous pouvez restaurer un système de fichiers UNIX ou Windows vers un disque partagé Windows pour les raisons suivantes :

- Si le système ne fait pas partie de la cellule Data Protector et ne dispose pas de l'Agent de disque Data Protector.
- Vous souhaitez effectuer des restaurations vers des plates-formes qui ne sont pas directement prises en charge par Data Protector, telles que les systèmes Windows pour Workgroups ou Windows 3.1.
- Vous souhaitez que les données soient disponibles sur plusieurs systèmes.

Lorsque vous restaurez les données vers un type de système de fichiers différent de celui à partir duquel elles ont été sauvegardées (d'un système UNIX vers un système Windows, par exemple), vous risquez de perdre les attributs spécifiques au système de fichiers.

Conditions préalables

Vous devez modifier le compte Inet Data Protector sur le client Agent de disque afin de disposer des autorisations appropriées pour accéder au disque partagé vers lequel vous souhaitez effectuer la restauration. Une autorisation d'accès au système client local et aux disques partagés distants doit être associée à ce compte. Il doit s'agir d'un compte utilisateur spécifique, et non du compte système.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, développez le type de données approprié.
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié.
4. Dans la page de propriétés Source, développez l'objet, puis sélectionnez les éléments à restaurer.
5. Cliquez sur l'onglet **Destination**.

6. Dans la liste déroulante **Client cible**, sélectionnez le système client Windows possédant l'Agent de disque à utiliser pour la restauration.

   CONSEIL :
   Vous pouvez ignorer les autres étapes si vous saisissez manuellement le chemin d'accès au réseau en spécifiant le nom de partage UNC du disque distant (*\\COMPUTER_NAME\SHARE_NAME*, par exemple, \\TUZLA\TEMP) dans la zone de texte **Restaurer vers nouvel emplacement**.

   Vous devez procéder ainsi si vous utilisez l'interface utilisateur sur un système UNIX, car le système n'est pas en mesure de confirmer l'existence d'un lecteur partagé Windows, ni de le rechercher. Vous devez donc confirmer vous-même que le lecteur est disponible et correctement spécifié pour éviter un échec de la sauvegarde.

7. Sélectionnez l'option **Restaurer vers nouvel emplacement** puis cliquez sur **Parcourir** pour afficher la boîte de dialogue **Explorer lecteurs**.
8. Développez **Réseau Microsoft Windows**, puis sélectionnez le disque partagé dans lequel vous souhaitez restaurer les données.
9. Cliquez sur **OK**.

Restauration d'objets en parallèle

La restauration en parallèle vous permet de restaurer en même temps des données provenant de plusieurs objets sur plusieurs disques ou systèmes de fichiers en ne lisant qu'une seule fois les supports. La restauration s'effectue alors encore plus rapidement.

Conditions préalables

Lors de la sauvegarde, les données provenant des différents objets doivent avoir été envoyées au même périphérique avec une simultanéité de 2 ou plus.

Limite

Il n'est pas possible de restaurer le même objet en parallèle. Par exemple, si vous sélectionnez le même objet de restauration sous **Restaurer objets** puis que vous sélectionnez ensuite la session qui contient le même objet sous **Sessions de restauration**, l'objet sera restauré une seule fois et un avertissement s'affichera.

Procédure

1. Sélectionnez les données comme vous le feriez pour une restauration simple. Vous pouvez également spécifier la destination de restauration, les options, etc.
2. Retournez dans le contexte Restauration dans la fenêtre de navigation, puis renouvelez l'étape 1 pour les données provenant des autres objets à restaurer.
3. Dans le menu **Actions**, cliquez sur **Démarrer restauration**. Un message vous indique que vous avez sélectionné plusieurs objets.
4. Activez l'option **Tous les objets sélectionnés (restauration en parallèle)**, puis cliquez sur

Suivant.

5. Testez votre sélection dans l'assistant de démarrage de session. Cliquez sur **Next**.
6. Spécifiez les options **Niveau de rapport**, **Charge réseau** et **Activer la reprise des restaurations**, puis cliquez sur **Terminer** pour lancer la restauration d'objets en parallèle.

Restauration d'une image disque

La restauration d'une image disque est une procédure de restauration rapide d'une sauvegarde d'image disque correspondante. Data Protector permet de restaurer la totalité de l'image d'un disque, secteur par secteur, au lieu de ne restaurer que les fichiers ou répertoires sélectionnés.

Pour restaurer une image disque UNIX ou Windows, développez l'objet l'élément **Image disque** dans le contexte Restauration, puis suivez la procédure de restauration standard.

Conditions préalables

- La sauvegarde à restaurer doit être du type image disque.
- Sur les systèmes UNIX, vous devez démonter le disque avant de procéder à la restauration de l'image disque, puis le remonter après la restauration en utilisant les commandes de pré- et post-exécution (par exemple, pré-exécution : `umount /dev/rdsk/disk1`, post-exécution : `mount /dev/rdsk/disk1 /mount_dir`).
- Si vous souhaitez restaurer une image disque sur un autre disque que celui à partir duquel vous avez effectué la sauvegarde, le nouveau disque doit être d'une capacité supérieure ou égale.

Restauration depuis des supports provenant d'un coffre

La restauration de données depuis un support provenant d'un coffre est similaire à la restauration depuis tout autre support. Selon la stratégie de protection du catalogue et des données adoptée, cependant, vous devrez peut-être exécuter des étapes supplémentaires :

- Si vous disposez d'une bibliothèque, entrez le support et analysez-le.
- Si la protection de catalogue est toujours valide pour le support, restaurez les données en sélectionnant celles que vous souhaitez restaurer à l'aide de l'interface utilisateur Data Protector.
- Si la protection de catalogue a expiré pour le support, Data Protector ne dispose d'aucune information détaillée sur les données sauvegardées. Restaurez les données en spécifiant manuellement les fichiers ou répertoires à récupérer

> **CONSEIL :**
> Pour relire les informations détaillées sur les fichiers ou répertoires à partir du support après l'expiration de la protection du catalogue, exportez le support, réimportez-le, puis spécifiez que vous souhaitez lire les données du catalogue des détails. Vous pourrez ensuite parcourir les fichiers et les répertoires via l'interface Data Protector.

Restauration d'un serveur Web

Pour restaurer un serveur Web, suivez la procédure de restauration standard pour la restauration des fichiers, des répertoires et des clients. Vous devez également tenir compte des points suivants :

- Toutes les données doivent être restaurées vers leur emplacement original.
- N'oubliez pas d'inclure les fichiers de configuration et les répertoires racine.
- Pour la restauration, le serveur Web doit être inactif, tandis que le système d'exploitation doit fonctionner. Après la restauration, vous devez redémarrer le serveur Web.

Si une base de données Oracle ou Informix est présente sur le serveur Web, suivez la procédure de restauration spécifique à la base de données.

Restauration sans exploration

Lorsque la protection du catalogue pour les données a expiré ou lorsque la sauvegarde a été effectuée à l'aide de l'option Pas de journalisation ou Journaliser répertoires, vous pouvez spécifier manuellement un fichier ou un répertoire à restaurer.

Si vous ne connaissez pas le nom d'un fichier ou d'un répertoire, vous pouvez restaurer la totalité de l'objet, puis extraire les parties qui vous intéressent, ou utiliser la fonction **Restaurer uniquement** pour ne restaurer que les fichiers correspondant à un modèle particulier, puis en extraire les parties souhaitées.

Restauration complète d'un objet et extraction des parties souhaitées

Lorsque vous ne pouvez pas explorer un fichier ou un répertoire à restaurer, vous pouvez restaurer l'objet dans son ensemble, puis extraire les données dont vous avez besoin.

Conditions préalables

Pour restaurer l'objet complet, vous devez disposer d'une quantité de mémoire temporaire aussi importante que l'objet lui-même.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié (par exemple **système de fichiers**).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié.
4. Cliquez sur l'onglet **Destination**. Sélectionnez un répertoire temporaire suffisamment volumineux pour stocker l'objet complet.
5. Spécifiez les options de votre choix dans les autres pages de propriétés de la restauration, notamment le périphérique à utiliser.

6. Dans le menu **Actions**, cliquez sur **Tester la restauration** si vous souhaitez exécuter un test ou sur **Démarrer la restauration** pour lancer effectivement le processus de restauration.
7. Dans l'assistant de démarrage de session, vérifiez votre sélection et spécifiez les options **Niveau de rapport**, **Charge réseau** et **Activer la reprise des restaurations**. Le moniteur de restauration affiche la progression de l'opération.
8. Une fois la restauration terminée, vous pouvez extraire de l'objet restauré les données dont vous avez besoin, puis les copier à l'endroit souhaité. Notez que cette opération s'effectue hors de Data Protector.

Restauration partielle d'un objet sauvegardé à l'aide du modèle de recherche Restaurer uniquement

Pour atteindre un fichier (ou le répertoire du niveau supérieur) ou un répertoire à restaurer que vous ne pouvez pas explorer, vous pouvez utiliser un modèle de recherche qui ne restaurera pas les parties non souhaitées de l'objet. Grâce aux caractères génériques, vous pouvez indiquer le modèle à utiliser.

> **REMARQUE :**
> Cette fonctionnalité n'est pas prise en charge par l'intégration de Data Protector avec le serveur NDMP.

Conditions préalables

- Pour que cette fonction donne de bons résultats, vous devez définir un modèle de recherche approprié.
- Vous devez disposer d'une mémoire temporaire pour les parties restaurées. La quantité de mémoire dépend de la taille des parties de l'objet restauré, et donc de la précision du modèle de recherche utilisé.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié (par exemple **système de fichiers**).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié.
4. Dans la page de propriétés Source, cliquez avec le bouton droit de la souris sur l'objet à partir duquel vous souhaitez effectuer la restauration, puis sélectionnez **Propriétés**.
5. Cliquez sur l'onglet **Restaurer uniquement**, puis, dans la zone de texte, spécifiez le modèle de recherche pour les fichiers à restaurer, par exemple, `*order*40*.ppt`, puis cliquez sur **Ajouter**. Il est conseillé d'ajouter plusieurs modèles afin de spécifier le plus précisément possible le type des fichiers à restaurer.
6. Cliquez sur **OK**.
7. Cliquez sur l'onglet **Destination**. Sélectionnez un répertoire temporaire suffisamment volumineux pour stocker les parties de l'objet sauvegardé.
8. Spécifiez les options de votre choix dans les autres pages de propriétés de la restauration,

notamment le périphérique à utiliser.

9. Dans le menu **Actions**, cliquez sur **Tester restauration** si vous souhaitez exécuter un test ou sur **Démarrer la restauration** pour lancer directement le processus de restauration.
10. Dans l'assistant de démarrage de session, vérifiez votre sélection et spécifiez les options Niveau de rapport, Charge réseau et Activer la reprise des restaurations. Le moniteur de restauration affiche la progression de l'opération. Si vous avez choisi le niveau de rapport "Avertissement", Data Protector émet un message d'avertissement car la liste de fichiers et de répertoires ne figure pas dans le catalogue de l'IDB. Néanmoins, la restauration n'en est pas affectée.
11. Une fois la restauration terminée, vous pouvez extraire de l'objet restauré les données nécessaires, puis les copier à l'emplacement souhaité. Notez que cette opération s'effectue hors de Data Protector.

Restauration manuelle de fichiers ou de répertoires

Lorsque vous ne pouvez pas explorer un fichier ou un répertoire à restaurer, vous pouvez le spécifier manuellement. Ceci se produit lorsque la protection de catalogue pour les données a expiré ou lorsque la sauvegarde a été effectuée à l'aide de l'option **Pas de journalisation**.

Conditions préalables

Pour ajouter manuellement un fichier ou un répertoire, vous devez connaître son chemin d'accès exact ainsi que son nom. Le nom du fichier et celui du chemin d'accès tiennent compte de la casse.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié (par exemple **système de fichiers**).
3. Développez le système client comportant les données à restaurer, puis, avec le bouton droit de la souris, cliquez sur l'objet contenant le fichier ou le répertoire à restaurer manuellement. Cliquez ensuite sur **Propriétés**.
4. Cliquez sur l'onglet **Résumé de restauration**, puis, dans la zone de texte, saisissez les parties manquantes du chemin d'accès et le nom du fichier ou du répertoire à restaurer.
5. Cliquez sur **Ajouter** pour confirmer. La fenêtre Version s'affiche.
6. Dans la liste déroulante Version, sélectionnez la version de sauvegarde à restaurer, puis cliquez sur **OK**. Le nom de l'objet ainsi que la version s'affichent.
7. Spécifiez les options de votre choix dans les autres pages de propriétés de la restauration, notamment le périphérique à utiliser.
8. Dans le menu **Actions**, cliquez sur **Tester la restauration** si vous souhaitez exécuter un test ou sur **Démarrer la restauration** pour lancer effectivement le processus de restauration.
9. Dans l'assistant de démarrage de session, vérifiez votre sélection et spécifiez les options **Niveau de rapport**, **Charge réseau** et **Activer la reprise des restaurations**.

Le moniteur de restauration affiche la progression de l'opération. Si vous avez choisi le niveau de rapport "Avertissement", Data Protector émet un message d'avertissement car la liste de fichiers et de répertoires ne figure pas dans le catalogue de l'IDB. Néanmoins, la restauration n'en est pas affectée.

Options de restauration

Data Protector propose un ensemble complet d'options de restauration qui permettent d'optimiser une restauration. Toutes ces options possèdent des valeurs par défaut adaptées à la plupart des situations.

Vous pouvez configurer les options suivantes objet par objet. Les options de restauration disponibles varient en fonction du type de données restaurées.

Pour plus d'informations sur les options de restauration, reportez-vous à Aide de HPE Data Protector.

Options de restauration générales

- **Afficher la chaîne complète.** Affiche l'intégralité des fichiers et répertoires de la chaîne de restauration. Par défaut, cette option est sélectionnée et toute la chaîne est restaurée.
- **Afficher cette session uniquement.** Affiche uniquement les fichiers et répertoires sauvegardés au cours de cette session. Vous pouvez ainsi restaurer les fichiers et répertoires d'une session de sauvegarde incrémentale sans avoir à restaurer l'intégralité de la chaîne de restauration. Cette option est désactivée par défaut.
- **Client cible.** Par défaut, vous restaurez vers le système client à partir duquel les données ont été sauvegardées. Vous pouvez sélectionner un autre système de la cellule dans la liste déroulante. L'Agent de disque est lancé sur le système client sélectionné, sur lequel les données sont restaurées.

  Vous devez disposer du droit utilisateur **Restaurer vers autres clients** pour pouvoir restaurer les données sur un autre système client.
- **Omettre les fichiers supprimés**. Pour que cette option fonctionne correctement, l'heure du Gestionnaire de cellule et celle du système où les données sont restaurées doivent être synchronisées.

  Si cette option est sélectionnée, Data Protector recrée l'état de la sauvegarde de l'arborescence de répertoires au moment de la dernière session de sauvegarde incrémentale, en conservant les fichiers qui ont été créés ou modifiés par la suite. Les fichiers supprimés entre la sauvegarde complète (la session initiale qui définit la chaîne de restauration) et la sauvegarde incrémentale choisie sont restaurés puis supprimés du fichier Restauration durant la restauration incrémentale ultérieure.

  Si cette option n'est pas sélectionnée, Data Protector restaure également les fichiers inclus dans l'image de sauvegarde complète et supprimés entre la sauvegarde complète (la session initiale qui définit la chaîne de restauration) et la sauvegarde incrémentale choisie.

  Lorsque vous utilisez la fonction **Restaurer sous** ou **Restaurer dans** avec cette option activée, choisissez soigneusement l'emplacement de restauration pour empêcher la suppression accidentelle de fichiers existants.

  Par défaut : désactivée.
- **Déplacer fichiers occupés.** Cette option concerne le cas où un fichier du disque est utilisé par une application alors qu'une restauration doit le remplacer. Elle ne s'applique qu'aux fichiers qui sont verrouillés par un système d'exploitation lorsqu'ils sont utilisés par l'application ou un autre processus. Vous pouvez utiliser cette option conjointement aux options **Garder le plus récent** ou **Ecraser**.

Cette option est désactivée par défaut.

Sur les systèmes UNIX, Data Protector déplace le fichier occupé en le renommant de `filename` en `#filename` (ajout d'un dièse devant le nom du fichier). L'application continue d'utiliser le fichier occupé jusqu'à sa fermeture. Le fichier restauré est ensuite utilisé.

Sous Linux, cette option n'est pas prise en charge.

Sous Windows, le fichier restauré s'appelle `filename.001.`. Toutes les applications continuent d'utiliser l'ancien fichier. Au redémarrage du système, l'ancien fichier est remplacé par celui restauré.

- **Lister données restaurées.** Affiche les noms des fichiers et répertoires dans la fenêtre du moniteur lors de la restauration des objets. Cette option est désactivée par défaut.
- **Afficher statistiques.** conserve des statistiques (comme la taille ou la performance) pour chaque objet sauvegardé ou restauré. Vous pouvez consulter ces informations dans la fenêtre du moniteur. Cette option est désactivée par défaut.
- **Omettre les versions d'objet non requises**. Cette option ne s'applique que si vous sélectionnez les répertoires pour la restauration et si la sauvegarde a été réalisée avec le niveau de journalisation **Journaliser tout** ou **Journaliser fichiers**.

  Si cette option est activée, Data Protector consulte l'IDB pour chaque sauvegarde de la chaîne de restauration, afin de vérifier s'il existe des fichiers à restaurer. Les sauvegardes sans versions d'objets à restorer sont ignorées. Notez que ces vérifications peuvent prendre un peu de temps.

  Si cette option est désactivée, chaque sauvegarde de la chaîne de restauration est lue, même s'il n'y a pas eu de modification depuis la précédente sauvegarde.

  Pour restaurer des répertoires vides, désactivez cette option.

  Par défaut : sélectionné.
- **Restaurer fichiers épars**. Restaure les fichiers épars dans leur format compressé d'origine. Les fichiers épars occupent de l'espace disque supplémentaire, sauf s'ils sont restaurés dans leur format d'origine. Cette option est désactivée par défaut.

  Cette option ne s'applique qu'aux fichiers épars UNIX. Les fichiers épars Windows sont toujours restaurés en tant que tels.
- **Verrouiller les fichiers pendant la restauration.** Refuse l'accès aux fichiers lors de la restauration. Cette option est désactivée par défaut.
- **Restaurer attributs de temps.** Permet de conserver les valeurs des attributs de temps de chaque fichier restauré. Si vous désactivez cette option, Data Protector définit les attributs de temps des objets restaurés en utilisant la date et l'heure courantes. Cette option est définie par défaut.
- **Restaurer attributs de protection.** Permet de conserver les attributs de protection d'origine de chaque fichier restauré. Si vous désactivez cette option, Data Protector utilise les attributs de protection de la session de restauration actuelle. Cette option est définie par défaut.

  Sur les systèmes Windows, cette option s'applique uniquement aux attributs de fichier. Les informations de sécurité sont toujours restaurées, même si cette option est désactivée.
- **Restauration des infos de partage pour les répertoires.** Spécifie que les informations partagées des répertoires seront restaurées. Par défaut, cette option est sélectionnée.

  Lors de la restauration d'un répertoire qui était partagé sur le réseau au moment de sa sauvegarde, ce répertoire sera également partagé après la restauration si cette option est sélectionnée, à condition que l'option **Sauvegarder les infos de partage des répertoires** ait été sélectionnée pour la sauvegarde.

Commandes de pré- et de post-exécution

- **Pré-exécution.** Permet d'entrer une commande (ou un script) à exécuter avant la restauration de chaque objet. Cette commande (ou ce script) doit renvoyer une réussite pour que Data Protector poursuive avec la restauration.

  La commande (ou le script) de pré-exécution est exécuté(e) sur le système client où l'agent de disque est exécuté. Sur un système Windows, les scripts doivent être situés dans le répertoire *Data_Protector_home*\bin, ou dans l'un des sous-répertoires de celui-ci. Sur les systèmes Unix, les scripts doivent être situés dans le répertoire /opt/omni/lbin, ou dans l'un des sous-répertoires de celui-ci.

  Notez que seules les extensions .bat, .exe et .cmd sont prises en charge pour les scripts de pré-exécution sur les systèmes Windows. Pour exécuter un script de pré-exécution avec une extension non prise en charge (par exemple .vbs), créez un fichier de commandes (.bat) qui démarre le script. Configurez Data Protector pour qu'il exécute le fichier de commandes comme une commande post-exécution, qui démarre ensuite le script avec l'extension non prise en charge.
- **Post-exécution.** Vous permet d'entrer une commande (ou un script) à exécuter avant la restauration de chaque objet. La commande (ou le script) post-exécution est exécuté(e) sur le système client où l'agent de disque est exécuté.

Sélection du périphérique

- **Sélection auto du périphérique.** Applicable lorsque les appareils d'origine ne sont pas disponibles pour un objet de restauration ou de copie. Sélectionnez cette option pour permettre à Data Protector de remplacer automatiquement les périphériques non disponibles avec d'autres périphériques sélectionnés pour la restauration ou copie d'objet et ayant le même marqueur de périphérique que celui d'origine. Si il n'y a pas assez de périphériques disponibles pour remplacer ceux d'origine, la restauration ou copie d'objet commence avec moins de périphériques que lors de la sauvegarde.

  Par défaut, Data Protector tente d'abord d'utiliser le périphérique d'origine. Si le périphérique d'origine n'est pas sélectionné pour une restauration ou une copie d'objet, alors une option globale est considérée. Pour utiliser d'abord des périphériques alternatifs ou empêcher l'utilisation du périphérique d'origine dans tous les cas, modifiez l'option globale AutomaticDeviceSelectionOrder.

  Pour l'intégration de Data Protector avec SAP MaxDB, DB2 UDB, Microsoft SQL Server et Microsoft SharePoint Server 2007/2010/2013, assurez-vous que le nombre d'appareils disponibles est supérieur ou égal au nombre de périphériques utilisés lors de la sauvegarde.

  Par défaut : sélectionné.
- **Sélection du périphérique d'origine**. Applicable lorsque les appareils d'origine ne sont pas disponibles pour un objet de restauration ou de copie pour le moment. Sélectionnez cette option pour indiquer à Data Protector d'attendre que les périphériques sélectionnés deviennent disponibles.

  Il s'agit de l'option conseillée pour l'intégration de Data Protector avec SAP MaxDB, IBM DB2 UDB, Microsoft SQL Server et Microsoft SharePoint Server 2007/2010/2013.

  Par défaut : désactivée.

Gestion des conflits de fichiers

- **Garder le plus récent.** Si vous sélectionnez cette option, les dernières versions des fichiers sont conservées. Si un fichier du disque est plus récent que la version sauvegardée, il n'est pas restauré. Si un fichier du disque est plus ancien que la version sauvegardée, il est écrasé par la nouvelle version de la sauvegarde. Cette option est définie par défaut.
- **Ne pas écraser.** Si vous sélectionnez cette option, les fichiers se trouvant sur le disque sont conservés. Dans ce cas, ils ne sont pas écrasés par d'autres versions provenant de la sauvegarde. Seuls les nouveaux fichiers sont restaurés à partir de la sauvegarde. Cette option est désactivée par défaut.
- **Ecraser.** Si vous sélectionnez cette option, les fichiers se trouvant sur le disque sont remplacés par ceux de la sauvegarde. Cette option est désactivée par défaut.

Options spécifiques d'Active Directory

Mode de réplication

- **Faisant autorité.** Cette option propre aux systèmes Windows Server concerne la restauration Active Directory. La base de données Active Directory n'est pas mise à jour après la restauration et les données restaurées écrasent celles existantes dans la destination cible. Pour effectuer une restauration en mode Faisant autorité, vous devez exécuter la commande `ntdsutil.exe` depuis l'invite de commande une fois la session de restauration terminée.
- **Ne faisant pas autorité.** La base de données Active Directory est mise à jour après la restauration à l'aide des techniques de réplication standard. Le mode de réplication **Ne faisant pas autorité** est défini par défaut.
- **Principale.** Le mode de réplication Principal permet de garder le service d'annuaire NT en ligne et de restaurer `FileReplicationService` en même temps que le service Active Directory. Vous devez utiliser cette option lorsque tous les partenaires de réplication d'un partage répliqué ont été perdus. Dans le cas de serveurs Certificate Server et Active Directory, **Principal** correspond à **Faisant autorité**.

Définition des options de restauration

Après avoir sélectionné les données à restaurer, vous pouvez définir les options de restauration. Ces options comportent des valeurs par défaut qui s'appliquent à la plupart des situations. Les options disponibles varient en fonction du type de données restaurées. Par exemple, vous ne disposez pas des mêmes options de restauration pour un système de fichiers et une image disque.

Procédure

1. Dans la liste de contexte, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, sous Restaurer objets, développez le type de données approprié (par exemple **système de fichiers**).
3. Développez le système client comportant les données à restaurer, puis cliquez sur l'objet approprié (point de montage pour des systèmes UNIX, lecteur pour des systèmes Windows).

4. Dans la page de propriétés Source, sélectionnez les données à restaurer.
5. Cliquez sur l'onglet **Options** pour ouvrir la page de propriétés Options. Pour activer ou désactiver une option, cliquez sur la case située en regard de celle-ci.

A propos de la restauration des systèmes Windows

Lors de la restauration d'un système de fichiers Windows, Data Protector restaure les données dans les fichiers et répertoires, ainsi que les informations spécifiques à Windows concernant les fichiers et les répertoires.

Les données propres à Windows restaurées sont les suivantes :

- Noms de fichier complets au format Unicode
- FAT16, FAT32, VFAT

  Attributs NTFS
- Autres flux de données.
- Informations partagées

  Si un répertoire est partagé sur un réseau au cours d'une sauvegarde, les informations partagées sont stockées sur le support de sauvegarde. Le répertoire doit être partagé sur le réseau après la restauration par défaut (sauf si un répertoire partagé associé au même nom de partage existe déjà). Pour éviter la restauration des informations partagées pour les répertoires, désélectionnez l'option Restaurer les informations de partage pour les répertoires.

  Les options de gestion des conflits de fichiers s'appliquent également à la restauration des informations partagées du répertoire. Par exemple, si l'option de restauration Ne pas écraser est utilisée pour la restauration, les informations partagées des répertoires figurant sur le disque sont préservées.
- Flux de données autres que NTFS
- Données de sécurité NTFS

Caractéristiques du système de fichiers NTFS 3.1

- Le système de fichiers NTFS 3.1 prend en charge les points d'analyse.

  Les points de montage de volume, le support de stockage unique (SIS) et les jonctions de répertoires se basent sur le concept des points d'analyse. Ces points sont sélectionnés comme tout autre objet de système de fichiers.
- Le système de fichiers NTFS 3.1 prend en charge les liens symboliques, qui sont une nouvelle fonction des systèmes d'exploitation Windows Vista et Windows Server 2008.

  Data Protector gère les liens symboliques de la même manière que les points d'analyse NTFS.
- Le système de fichiers NTFS 3.1 prend en charge les fichiers épars, ce qui permet de réduire efficacement la quantité d'espace disque allouée.

  Ces fichiers sont sauvegardés de manière éparse afin d'économiser de la place sur les bandes. Les fichiers épars sont sauvegardés et restaurés de manière éparse uniquement sur le système de fichiers NTFS 3.1.
- Certaines fonctions spécifiques au système de fichiers NTFS 3.1 sont contrôlées par les services du système qui maintiennent leurs propres enregistrements de données. Les structures de données

sont sauvegardées en tant que partie d'une sauvegarde CONFIGURATION.

- Fichiers cryptés

  Les fichiers NTFS 3.1 cryptés via des applications Microsoft sont sauvegardés et restaurés cryptés, mais leur contenu ne peut être correctement affiché qu'après décryptage.
- Les fichiers compressés sont sauvegardés et restaurés sous forme compressée.

Tenez compte des limites de la restauration des systèmes de fichiers lors de la restauration vers un type de système de fichiers différent de celui sur lequel la sauvegarde a été effectuée.

Restauration d'objets sauvegardés en tant que disques partagés

Les objets sauvegardés en tant que disques partagés sont associés au client Agent de disque qui a servi à leur sauvegarde. Si l'environnement n'a pas changé, vous pouvez restaurer les disques partagés comme s'il s'agissait d'un système de fichiers Windows local. Par défaut, le client Agent de disque qui a servi à sauvegarder les disques partagés est également utilisé pour restaurer les données vers l'emplacement d'origine.

Limites de la restauration de systèmes de fichiers Windows

Vous pouvez restaurer les données vers un autre type de système de fichiers que celui sur lequel la sauvegarde a été effectuée.

De	**A**				
	FAT32	FAT16	CDFS	UDF	NTFS 3.1 [1]
FAT32	FC	FC	Sans objet	Sans objet	FC
FAT16	FC	FC	Sans objet	Sans objet	FC
CDFS	FC	FC	Sans objet	Sans objet	FC
UDF	FC	FC	Sans objet	Sans objet	FC
NTFS 3.1 [2]	*	*	Sans objet	Sans objet	FC

Légende	
FC	Compatibilité totale : tous les attributs de fichiers sont conservés.
*	Les points d'analyse, les fichiers épars et les fichiers cryptés ne sont pas restaurés. Les fichiers sont restaurés sans les informations de sécurité et les autres flux de données.

[1] Utilisé sous Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008 et Windows Server 2012.
[2] Utilisé sous Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008 et Windows Server 2012.

Ce tableau montre que les objets du système de fichiers NTFS 3.1 ne peuvent être correctement restaurés que vers le système de fichiers NTFS 3.1. Les attributs propres au système de fichiers et les autres flux de données sont perdus lors de la restauration vers une version différente du système de fichiers.

- Les points d'analyse Windows, par exemple une jonction de répertoires ou un point de montage de volume, peuvent uniquement être restaurés vers un système de fichiers NTFS 3.1. Les points d'analyse UNIX ne peuvent pas être restaurés vers un système de fichiers NTFS 3.1.
- Lorsque vous restaurez un système de fichiers NTFS 3.1 contenant des points d'analyse SIS, une situation de "disque plein" peut se produire. Tel est le cas si le fichier d'origine est restauré vers plusieurs fichiers cibles qui occupent plus d'espace que celui disponible.
- Les fichiers épars sont restaurés en tant que tels uniquement sur le système de fichiers NTFS 3.1.
- Data Protector ne permet pas de restaurer les quotas de disque utilisateur.
- Si un utilisateur tente de restaurer un fichier épars vers un système de fichiers autre que NTFS 3.1, Data Protector affiche un message d'avertissement. Un fichier épars restauré vers un système de fichiers autre que NTFS 3.1 ne comporte pas de sections nulles.
- Les fichiers NTFS 3.1 cryptés via des applications Microsoft peuvent être restaurés uniquement vers le système de fichiers NTFS 3.1 car les autres pilotes de systèmes de fichiers ne peuvent pas les décrypter.

Restauration d'une configuration

Pour restaurer la CONFIGURATION de Windows, sélectionnez l'objet `CONFIGURATION` ou certaines de ses parties et suivez la procédure de restauration standard.

La CONFIGURATION est composée de structures de données qui ont une influence sur le fonctionnement du système. Ainsi, le système doit être préparé pour une telle restauration. Les conditions prérequises dépendent du contenu de l'élément CONFIGURATION et de la version du système d'exploitation Windows.

Limites

- Le service Active Directory et SysVol doivent être restaurés ensemble.
- Data Protector ne permet pas de restaurer les quotas de disque utilisateur. Les informations sauvegardées peuvent être restaurées manuellement, à l'aide des utilitaires Microsoft.
- Même si Data Protector vous permet de restaurer des objets de configuration uniques, il n'est **pas conseillé** de le faire. Il est fortement recommandé d'effectuer une restauration de configuration complète dans le cadre de la procédure de **Récupération après sinistre**.

Objets de configuration Windows

Pour plus d'informations sur les objets de configuration, reportez-vous à Aide de HPE Data Protector.

- Service Active Directory
- Certificate Server
- Base de données d'enregistrement des classes COM+ (`ComPlusDatabase`)
- DFS

- DHCP
- Serveur DNS
- Journaux d'événements
- Service de réplication de fichiers
- Internet Information Server (IIS)
- Profils utilisateur (`Documents and Settings`)
- Registre Windows
- Base de données du gestionnaire de supports amovibles
- SystemRecoveryData
- SysVol
- Base de données des services Terminal Server
- Quotas de disque utilisateur (`QuotaInformation`)
- serveur WINS

Redémarrez le système après la restauration de l'objet CONFIGURATION complet afin que les données restaurées entrent en effet.

Certains objets nécessitent des considérations et tâches spéciales.

Active Directory

Pour restaurer le service Active Directory, vous devez redémarrer le système en utilisant l'option de démarrage Mode restauration des services d'annuaire. Lorsque le système est démarré en Mode restauration des services d'annuaire, les comptes d'utilisateur du domaine ne peuvent pas être utilisés. Vous devez configurer Data Protector Inet et le service `crs` (pour un Gestionnaire de cellule) pour vous connecter avec le compte système local, puis redémarrer les services. Lors de la restauration de l'Active Directory, le service de réplication des fichiers (FRS) et le système de fichiers distribués (DFS) sont également restaurés.

Vous pouvez restaurer l'Active Directory dans un des trois modes de réplication (options propres à Windows) :

- ne faisant pas autorité
- faisant autorité
- principal

> **REMARQUE :**
> Pour effectuer une restauration **Faisant autorité**, vous devez également exécuter `ntdsutil.exe` une fois la session de restauration terminée. Par exemple, pour effectuer une restauration faisant autorité typique, saisissez `ntdsutil` dans une invite de commande, puis `authoritative restore`, restaurez alors la base de données. Redémarrez le serveur et attendez que la réplication ait lieu.

> **CONSEIL :**
> Vous pouvez également créer une commande post-exécution pour exécuter l'action supplémentaire nécessaire pour la restauration Active Directory faisant autorité. Par exemple, pour effectuer une restauration faisant autorité d'un répertoire entier, utilisez la ligne suivante :

```
ntdsutil "popups off" "authoritative restore" "restore database" quit quit
```

DFS

Data Protector restaure le système de fichiers distribués (DFS) Windows en même temps que l'un des éléments suivants :

- Registre Windows, si le DFS est configuré en mode autonome
- Windows Active Directory, si le DFS est configuré en mode de domaine

Profilage

- Un profil utilisateur ne peut pas être restauré correctement si l'utilisateur concerné est connecté, de façon interactive ou en tant que service. Si l'utilisateur est connecté au moment de la restauration, Data Protector ne pourra pas restaurer le fichier `NTUSER.DAT` contenant la "ruche" du registre de l'utilisateur.

  Vous devez vous déconnecter du système et arrêter tous les services qui sont exécutés sous le compte utilisateur dont vous souhaitez restaurer les profils. La session de restauration peut être démarrée à partir d'un autre système ou en vous connectant sur le système cible de la restauration avec un autre nom d'utilisateur.
- Pour restaurer tous les profils utilisateur à la fois, vous devez arrêter les services qui ne sont pas exécutés par le compte système local, et vous déconnecter du système. Puis démarrez la session de restauration à distance, avec l'interface graphique Data Protector sur un autre client.
- Un profil utilisateur ne peut être restauré que lorsque son emplacement est déjà défini sur le système. Les fichiers individuels de profils utilisateur existants ou de profils supprimés peuvent encore être restaurés tant qu'ils existent parmi les profils du système. Si un profil utilisateur a été supprimé depuis le Panneau de configuration, ou que le profil de l'utilisateur n'existe plus sur le système pour une autre raison, la restauration échoue avec l'erreur suivante :

  ```
  [84:208] Configuration object not recognized by the system => not restored.
  ```

  Pour restaurer un tel profil utilisateur, vous devez d'abord le recréer en vous connectant avec les identifiants de cet utilisateur. Le système attribue un répertoire pour le profil de l'utilisateur et crée un profil par défaut. Pour garder les fichiers restaurés en état non fusionné, vous pouvez supprimer les fichiers du profil nouvellement créé avant de lancer une session de restauration. Puis déconnectez-vous et redémarrez la session en vous connectant avec un autre compte utilisateur ou avec un autre système. Le système peut attribuer un nom différent à l'utilisateur. Dans ce cas, utilisez l'option **Restaurer sous** pour restaurer les fichiers vers l'emplacement nouvellement affecté.
- Lorsque les profils utilisateur sont restaurés, les fichiers sont toujours écrasés, quelles que soient les options de gestion des conflits de fichiers dans la spécification de restauration. De plus, l'option **Omettre les fichiers supprimés** n'est pas disponible. Les fichiers qui existent sur le disque mais qui n'étaient pas présents au moment de la sauvegarde resteront dans le profil utilisateur après la restauration.
- Les profils utilisateur peuvent également être restaurés avec l'option **Restaurer sous**. Vous pouvez spécifier un emplacement temporaire pour les fichiers puis copier manuellement les fichiers souhaités vers le répertoire du profil utilisateur. Vous pouvez également restaurer directement dans le répertoire du profil de l'utilisateur, en utilisant éventuellement l'option **Déplacer fichiers occupés**, qui vous permet de restaurer un profil utilisateur même s'il est utilisé par un utilisateur connecté.

Notez cependant que dans ce cas, les fichiers en cours d'utilisation ne seront remplacés qu'après le redémarrage du système.

Registre

Si vous sélectionnez le `Windows Registry` complet pour une restauration, certaines des clés de registre ne sont pas restaurées et certaines sont traitées de façon particulière lors d'une restauration. La raison de ce fonctionnement est que les clés sont utilisées par le système d'exploitation. Vous pouvez les trouver sous la clé de registre suivante :

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\KeysNotToRestore`

Base de données du gestionnaire de supports amovibles

Le service RSM doit être exécuté sur tous les systèmes avec des supports de stockage amovibles connectés (hors CD-ROM).

Objets de configuration du serveur

Le système cible doit disposer du serveur correspondant installé et en cours d'exécution. Pour tous les serveurs, en dehors du serveur de certificats, les données sont restaurées en ligne.

Les données du serveur de certificats sont restaurées hors ligne. Arrêtez les services du serveur de certificats avant de lancer une restauration. Vous pouvez restaurer le serveur de certificats uniquement avec le mode faisant autorité.

SysVol

Vous pouvez effectuer la restauration du répertoire SysVol dans un des trois modes suivants :

- ne faisant pas autorité

  Si au moins un contrôleur de domaine dans le domaine est disponible et en cours d'exécution, les fichiers sont restaurés à leur emplacement d'origine. Les données restaurées ne sont pas propagées aux autres contrôleurs de domaine.
- faisant autorité

  Effectuez une restauration faisant autorité si des données SysVol critiques sont supprimées du contrôleur de domaine local et que la suppression est propagée à d'autres contrôleurs de domaine.
- principal

  Si tous les contrôleurs de domaine du domaine sont perdus et que vous voulez recréer le contrôleur de domaine depuis la sauvegarde, le FRS est informé que vous restaurez des fichiers essentiels, et les fichiers sont restaurés à leur emplacement d'origine.

Services TCP/IP Windows

Sur un système Windows qui exécute un protocole TCP/IP Microsoft et est configuré comme serveur WINS, DHCP ou DNS, vous pouvez restaurer les services qui gèrent les communications réseau.

Pour restaurer les services TCP/IP Windows, développez l'élément CONFIGURATION et sélectionnez WNS, DHCP ou DNSServerDatabase.

Chacun de ces services est automatiquement arrêté avant la restauration.

Une fois la restauration terminée, redémarrez le système.

Restauration des données d'état du système

Si vous utilisez Active Directory, qui fait toujours partie de l'état du système, vous devez démarrer le système en mode restauration Directory Services.

Du point de vue de Data Protector, l'état du système se compose d'objets spécifiques du système de fichiers et d'objets CONFIGURATION. Sous Windows Vista, Windows 7, Windows 8, Windows Server 2008 et Windows Server 2012, l'état du système inclut également des données appartenant à d'autres rôles serveurs ou services éventuellement installés. Contrairement à la sélection d'objets dans l'assistant de sauvegarde, les différents objets à restaurer doivent être sélectionnés dans des assistants de restauration distincts.

Dans la page de propriétés Source, sélectionnez les éléments suivants :

- les objets d'état du système de type CONFIGURATION :
  - ActiveDirectoryService
  - CertificateServer
  - Cluster Service information
  - IIS Metadirectory
  - RemoteStorageService
  - RemovableStorageManagementDatabase
  - SystemFileProtection
  - SYSVOL directory
  - TerminalServiceDatabase
- SystemVolumeInformation (y compris le service de protection des fichiers système)
- Fichiers d'amorçage (qui se trouvent sur le lecteur système)
- Volumes comportant des données appartenant à des rôles serveurs ou des services, voire l'intégralité du système client (dans le cas d'un système Windows Vista, Windows 7, Windows 8, Windows Server 2008 et Windows Server 2012)

Une fois la restauration terminée, redémarrez le système.

Service de stockage distant (RSS - Remote Storage Service)

Le service de stockage distant permet de déplacer automatiquement les fichiers peu utilisés de l'emplacement de stockage local à l'emplacement de stockage distant. Les fichiers distants sont

rappelés automatiquement à leur ouverture.

Bien que les bases de données RSS fassent partie des données d'état du système, vous pouvez les restaurer manuellement. La restauration des bases de données RSS doit s'effectuer hors ligne. Vous pouvez faire appel à des scripts de pré- et de post-exécution pour arrêter et redémarrer le service, ou effectuez ces tâches manuellement avant et après la restauration.

Sélectionnez les répertoires suivants pour la restauration :

%SystemRoot%\system32\RemoteStorage

%SystemRoot%\system32\NtmsData

Protection de fichiers système

Le service de protection des fichiers système analyse et vérifie les versions de tous les fichiers système protégés après le redémarrage de votre ordinateur. Si le service de protection des fichiers système découvre qu'un fichier protégé a été écrasé, il récupère la version correcte de celui-ci et remplace le fichier incorrect. Data Protector permet de sauvegarder, puis de restaurer des fichiers protégés sans les écraser.

A propos de la restauration des systèmes UNIX

En cas de restauration de fichiers vers l'emplacement d'origine à partir duquel la sauvegarde a été réalisée, Data Protector restaure également les attributs de fichier.

Les données propres au système, comme par exemple les ACL (listes de contrôle d'accès) dans des systèmes UNIX, ne peuvent être restaurées que sur le même type de système de fichiers et le même système d'exploitation que ceux de la sauvegarde.

Données propres aux systèmes UNIX

Pour la restauration des données VxFS, utilisez l'option Restaurer sous, puis restaurez les données vers l'emplacement souhaité.

A propos de la Restauration du Système HP OpenVMS

Utilisez la procédure de restauration classique pour restaurer les systèmes de fichier HP OpenVMS.

Limites

- Pour les fichiers et répertoires enregistrés sur toute autre plate-forme de système d'exploitation, tous les attributs de fichiers ne sont pas restaurés et aucune ACL n'est restaurée dans ce cas.
- Les répertoires qui sont créés pendant une restauration mais n'ont pas été inclus dans une sauvegarde obtiendront les attributs du premier fichier restauré dans le répertoire, à moins qu'ils ne soient désactivés par l'option `-no_protection`.
- Les spécifications de fichiers saisies dans l'interface graphique ou transmises à l'interface de ligne de commande doivent respecter la syntaxe de style UNIX

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

La chaîne doit commencer par une barre oblique, suivie par le disque, les répertoires et le nom du fichier, séparés par des barres obliques.

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 fichier pour les fichiers OpenVMS ne sont pas sensibles à la casse. Par exemple, une spécification de fichier OpenVMS :

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

doit être spécifiée sous la forme :

```
/$1$DGA100/Users/Doe/Login.Com.1
```

- Il n'y a pas de numéro de version implicite. Vous devez toujours spécifier un numéro de version. Seules les versions de fichier sélectionnées pour la restauration seront restaurées. Si vous souhaitez inclure toutes les versions du fichier, sélectionnez-les toutes dans la fenêtre de l'interface graphique, ajoutez les spécifications de fichier sous l'option **Uniquement** (`-only`) en intégrant des caractères génériques pour le numéro de version, comme suit :

  ```
  /DKA1/dir1/filename.txt.*
  ```
- Si vous restaurez vers un emplacement autre que celui d'origine, seul le périphérique de disque et le répertoire de départ sont modifiés. Le chemin d'origine vers le répertoire est ajouté au chemin de destination afin de former le nouvel emplacement de restauration.
- Si l'option **Restaurer les Attributs Temporels** (`-notouch`) est désactivée pendant une restauration, la date du dernier accès sera actualisée avec la date et l'heure actuelles sur les disques ODS-5. Sur les disques ODS-2, les dates d'origine seront définies pour les fichiers.
- Un fichier sauvegardé comme lien soft sera restauré à l'aide de l'équivalent d'une commande `DCL SET FILE/ENTER`. Aucune donnée ne sera restaurée dans ce cas. Les points de lien symbolique entrés vers le chemin/nom de fichier principal pour ce fichier au moment de l'enregistrement du fichier. Si le chemin/nom de fichier principal n'existe pas ou n'a pas été restauré, la création du lien symbolique échouera.

  Pour rendre une copie restaurée d'un disque système amorçable, l'utilitaire OpenVMS WRITEBOOT a été utilisé pour écrire un bloc d'amorçage une fois le disque restauré.
- Les options **Déplacer les Fichiers Actifs** (`-move`) et **Restaurer les Fichiers Fragmentés** (`-sparse`) ne sont pas disponibles sur OpenVMS.
- Les fichiers sauvegardés d'un disque ODS-5 sur un système OpenVMS ayant des noms de système de fichiers étendus (c'est-à-dire des lettres majuscules et minuscules, des caractères Unicode et ainsi de suite) peuvent ne pas être restaurés sur un disque ODS-2.
- Les fichiers étant restaurés sont toujouts verrouillés peu importe si l'option **Verrouiller Fichiers pendant la Restauration** (`-lock`) est activée ou désactivée.
- Le périphérique et le répertoire par défaut pour les procédures de commande pré et post-exécution est `/omni$root/bin`. Pour placer la procédure de commande à un autre endroit, la spécification de fichier doit contenir le chemin du périphérique et du répertoire au format UNIX. Par exemple :

  ```
  /SYS$MANAGER/DP_SAVE1.COM
  ```
- Si l'option **Restaurer les Attributs de Protection** (`-no_protection`) est désactivée, les fichiers sont créés avec le titulaire par défaut, la protection et l'ACL.
- Lorsque vous indiquez les caractères de la carte de remplacement pour l'utilisation des filtres **Passer** (`-skip`) ou **Uniquement** (`-only`) '*' pour des caractères multiples et '?' pour des caractères

simples.

- Sur les systèmes OpenVMS, Data Protector ne prend pas en charge les quotas de disque sur les volumes et les jeux de volumes.

  Pour effectuer la restauration de données situées sur un volume avec un quota de disque activé, configurez le script de post-exécution pour qu'il désactive le quota de disque sur le volume concerné avant le début de la restauration, et configurez le script de pré-exécution pour qu'il active le quota de disque après la restauration.

Informations du système de fichiers restaurées

La structure de répertoires et les fichiers suivants sont restaurés, avec les informations suivantes sur le système de fichiers :

- Attributs des fichiers et des répertoires
- ACL (listes de contrôle d'accès) si disponibles (voir Limites)
- Entrées de fichier secondaires

  Lors d'une sauvegarde du système de fichiers OpenVMS, les fichiers avec plusieurs entrées de répertoire sont sauvegardés une fois en utilisant le nom chemin d'accès principal. Les entrées de chemin secondaires sont enregistrées en tant que liens symboliques.

  Par exemple, les racines spécifiques du système sur un disque système OpenVMS auront le chemin mémorisé `SYSCOMMON.DIR;1` comme lien symbolique. Les données de ce chemin seront enregistrées sous `[VMS$COMMON...]`.

  Lors d'une restauration du système de fichiers, ces entrées de chemin supplémentaires sont restaurées.

Les fichiers peuvent être restaurés vers les volumes installés `FILES-11`, `ODS-2` ou `ODS-5` uniquement.

Chapitre 15: Surveillance, rapports, notifications et Data Protector journal d'événements

A propos de la surveillance

Data Protector permet de gérer les sessions en cours d'exécution et de répondre à des demandes de montage. Vous pouvez consulter l'état des sessions, leur type, leur propriétaire, leur ID de session, ainsi que l'heure de début des sessions et le nom des spécifications de sauvegarde correspondantes.

Lorsque vous exécutez une session interactive de sauvegarde, restauration, copie d'objet, consolidation d'objet, vérification d'objet ou de gestion de supports, une fenêtre de contrôle s'ouvre affichant les objets, les périphériques de sauvegarde et les messages générés durant la session. Même si l'interface utilisateur est fermée, la session se poursuit.

Vous pouvez modifier le niveau des messages transmis au cours d'une session de sauvegarde ou de restauration en modifiant l'option **Niveau de rapport** lors de la configuration d'une spécification de sauvegarde ou au démarrage d'une session de restauration.

Vous pouvez surveiller plusieurs cellules simultanément à l'aide de la fonction Manager-of-Managers.

Affichage des sessions en cours

Vous pouvez afficher les sessions en cours d'exécution dans le contexte Moniteur.

> **REMARQUE :**
> Une session en cours d'exécution est affichée dans le contexte Moniteur une fois le script de pré-exécution terminé.
>
> La liste des sessions en cours est automatiquement mise à jour selon l'intervalle d'actualisation défini (5 secondes par défaut). Pour modifier l'intervalle d'actualisation par défaut, cliquez sur **Préférences** dans le menu Fichier, puis sélectionnez l'onglet Moniteur. Vous pouvez indiquer l'intervalle d'actualisation en secondes pour le Gestionnaire de cellule et pour le Gestionnaire MoM.

Conditions préalables

Vous devez être membre du groupe d'utilisateurs Admin ou disposer des droits utilisateur Moniteur.

Procédure

1. Dans la liste de contexte, cliquez sur **Moniteur**.
   La zone de résultats affiche l'état des sessions en cours.

   > **CONSEIL :**
   > Vous pouvez trier les sessions (par `status`, `type`, `owner`, etc.) en cliquant sur l'en-tête de

> colonne correspondant. Pour l'intégration de VMware, vous pouvez trier les sessions par `VM name` et `item name` également. Ici, `VM name` désigne le nom de la machine virtuelle dans vCenter et `item name` désigne le nom de la configuration ou de l'objet de disque associé(e) à la machine virtuelle.

2. Double-cliquez sur la session en cours à visualiser.

> **CONSEIL :**
> Pour supprimer toutes les sessions terminées ou abandonnées dans la zone de résultats du contexte Moniteur, cliquez sur **Sessions en cours** dans la fenêtre de navigation, puis sélectionnez **Effacer les sessions** dans le menu Actions. Pour supprimer une session terminée ou abandonnée de la liste des sessions en cours, cliquez avec le bouton droit sur la session en question et sélectionnez **Supprimer de la liste**. Toutes les sessions terminées ou abandonnées sont automatiquement supprimées de la zone de résultats du contexte Moniteur si vous redémarrez l'interface Data Protector.

Affichage des sessions terminées

Vous pouvez afficher les sessions terminées ou abandonnées dans le contexte Base de données interne.

Conditions préalables

Vous devez faire partie du groupe d'utilisateurs Admin ou disposer des droits d'utilisateur Moniteur.

Procédure

1. Dans la liste de contexte, cliquez sur **Base de données interne**.

   Si vous exécutez Manager-of-Managers, sélectionnez **Moniteur** dans la liste de contexte, puis sélectionnez le Gestionnaire de cellule souhaité. Dans le menu Outils, sélectionnez **Administration base de données** pour ouvrir une nouvelle interface Data Protector dans laquelle apparaît le contexte de base de données interne sélectionné.
2. Dans la fenêtre de navigation, développez **Sessions** pour afficher toutes les sessions stockées dans l'IDB. Les sessions sont triées par date. Chaque session est identifiée par un ID composé d'une date au format JJ/MM/AA et d'un numéro unique.
3. Cliquez avec le bouton droit sur la session, puis sélectionnez **Propriétés** pour afficher les détails d'une session donnée.
4. Cliquez sur l'onglet **Général**, **Messages** ou **Media** pour afficher respectivement les informations concernant la session, les messages de session ou les supports utilisés pour cette session.

Abandon de sessions en cours

Pour interrompre une opération de sauvegarde, restauration ou gestion des supports, vous devez abandonner la session en cours. Une copie de sauvegarde ou des données restaurées contiendront uniquement les données sauvegardées ou restaurées avant l'abandon de la session.

Conditions préalables

Vous devez faire partie du groupe d'utilisateurs `admin` ou disposer des droits d'utilisateur Moniteur.

Procédure

1. Dans la liste de contexte, cliquez sur **Moniteur**. L'évolution et l'état des sessions en cours s'affichent dans la zone de résultats.

   Si vous exécutez un Manager-of-Managers, développez le **Moniteur d'entreprise** dans la fenêtre de navigation, puis sélectionnez le Gestionnaire de cellule à surveiller. L'évolution et l'état des sessions en cours s'affichent dans la zone de résultats.
2. Pour trier les sessions, cliquez sur les en-têtes des colonnes.
3. Cliquez avec le bouton droit sur la session et sélectionnez **Abandonner**.

Si vous abandonnez une session de sauvegarde alors que le logiciel est encore en train de déterminer la taille des disques que vous avez sélectionnés, la sauvegarde n'est pas abandonnée immédiatement. L'abandon est effectif une fois la taille (parcours arborescent) déterminée.

> **CONSEIL :**
> Si vous avez démarré une session de sauvegarde, de restauration ou de gestion des supports de façon interactive, vous pouvez aussi utiliser, respectivement, les contextes Sauvegarde, Restauration ou Périphériques et supports de Data Protector.

À propos de la génération de rapports

Les rapports Data Protector fournissent diverses informations sur votre environnement de sauvegarde. Vous pouvez, par exemple, vérifier l'état de la dernière sauvegarde, copie d'objets, consolidation d'objet ou vérification d'objet, vérifier les systèmes de votre réseau qui ne sont pas configurés pour une sauvegarde, vérifier la consommation de supports dans les pools de supports, vérifier l'état des périphériques, etc.

Vous pouvez configurer des groupes de rapports et des rapports à l'aide de l'interface Data Protector ou de tout navigateur Web supportant Java. Les groupes de rapports permettent de gérer facilement les rapports, de les planifier dans les groupes de rapports et de définir les critères de regroupement des rapports dans ces groupes.

Les paramètres vous permettent de personnaliser les rapports. Vous pouvez effectuer des sélections multiples avec certains paramètres. Si aucun paramètre d'entrée facultatif n'est spécifié lors de la configuration d'un rapport, une valeur par défaut est définie : *`all`* dans le cas d'objets et *`no time limit`* dans le cas de périodes. Pour configurer un rapport ou un groupe de rapports, vous devez fournir :

- un nom pour le rapport ;
- le type du rapport ;
- la méthode d'envoi ;
- le/les destinataires ;
- le format.

Tous les autres paramètres d'entrée (sélections) dépendent du type de rapport.

> **REMARQUE :**
> La fonctionnalité de rapport VADP est activée par défaut. Pour la désactiver, définissez la variable globale `EnableDPAforVM` sur `0`.

Fonctions

- Vous pouvez regrouper plusieurs rapports dans un groupe de rapports, qui peuvent être planifiés, lancés de manière interactive ou déclenchés par une notification.
- Les rapports peuvent être lancés à l'aide de l'interface utilisateur de Data Protector, de la ligne de commande de Data Protector, du planificateur de Data Protector, d'un événement de notification ou d'un script de post-exécution contenant une commande de ligne de commande de Data Protector qui déclenche la génération du rapport.
- La génération de rapports est également disponible pour une configuration multicellules lorsque vous utilisez la fonction Manager-of-Managers (MoM).
- La sortie des rapports est fournie en plusieurs formats et peut également afficher les paramètres d'entrée (sélections).

Formats de rapports

Vous pouvez générer des rapports Data Protector sous divers formats.

Si vous lancez chaque rapport individuellement, il s'affiche dans le Gestionnaire Data Protector et vous n'avez pas besoin de choisir de format de rapport.

Si vous rassemblez des rapports dans des groupes de rapports, vous devez préciser le format et les destinataires de chaque rapport.

Vous pouvez choisir parmi les formats de rapports suivants :

- **ASCII** - Un rapport est généré sous la forme de texte brut.
- **HTML** - Un rapport est généré au format HTML. Ce format est utile pour la consultation via un navigateur Web. Vous pouvez par exemple vérifier si vos systèmes ont été sauvegardés en cliquant sur un lien et en consultant le rapport sur l'intranet.
- **Court** - Un rapport est généré sous la forme d'un résumé en texte brut présentant les informations les plus importantes. Ce format est proposé pour les messages de diffusion.
- **Tab** - Un rapport est généré avec des champs séparés par des tabulations. Ce format est utile pour l'importation de rapports dans d'autres applications ou scripts pour des analyses ultérieures, comme Microsoft Excel.

Le résultat réel d'un rapport varie selon le format sélectionné. Seul le format Tab affiche tous les champs pour tous les rapports, les autres formats pouvant parfois n'afficher que les champs sélectionnés.

Types de rapports

Selon les informations dans votre environnement de sauvegarde que vous voulez récupérer, vous pouvez générer plusieurs types de rapports :

Rapports de configuration

Les rapports de configuration fournissent des informations sur la configuration de la cellule Data Protector, sur les périphériques non utilisés pour la sauvegarde, sur les systèmes non configurés pour la sauvegarde, etc.

Informations sur la cellule

Description :	Répertorie des informations concernant la cellule Data Protector (nombre de clients, spécifications de sauvegarde, serveur de gestion des supports, serveur de licences). La caractéristique VADP adoptée par Data Protector 8.14 offre des rapports améliorés pour les machines virtuelles. Les machines virtuelles VMware sont représentées comme des clients Data Protector, appelés clients VADP. Les clients VADP affichent les informations relatives au système d'exploitation invité de la machine virtuelle. Si les outils VM sont installés et en cours d'exécution et que VM est sous tension, la section des informations d'hôte affiche des informations telles que le système d'exploitation, l'adresse IP ou le nom d'hôte. Le nom d'hôte VM doit afficher le nom DNS, s'il est configuré sur une machine virtuelle. Le nom d'hôte VM doit afficher l'adresse IP, si VM ne comporte pas de nom DNS et que l'adresse IPv4 est disponible. Le nom d'hôte VM doit afficher le nom VM, si ne nom DNS ou l'adresse IP n'est pas disponible ou si la machine virtuelle ne dispose que de l'adresse IPv6.
Sélections requises :	aucune
Sélections facultatives :	aucune
Formats pris en charge :	tous les formats
option omnirpt :	`cell_info`

Sauvegarde de client

Description :	Répertorie des informations sur les clients spécifiés, comme : systèmes de fichiers non configurés, tous les objets, tous les objets avec une sauvegarde valide et leurs heures de sauvegarde et tailles moyennes. Notez que les rapports Sauvegarde de client n'incluent pas d'informations sur les objets sauvegarde d'intégration d'application et les spécifications de sauvegarde.

Sélections requises :	hostname
Sélections facultatives :	aucune
Formats pris en charge :	tous les formats
option omnirpt :	`host`

Clients non configurés pour Data Protector

> **REMARQUE :**
> La création de ce rapport peut prendre du temps, en fonction de la condition du réseau. La création de ce type de rapport ne peut pas être abandonnée.

Description :	Répertorie les clients dans les domaines sélectionnés qui ne font pas partie de la cellule actuelle.
Sélections requises :	plage(s) réseau
Sélections facultatives :	aucune
Formats pris en charge :	tous les formats
option omnirpt :	`hosts_not_conf`

Clients configurés non utilisés par Data Protector

Description :	Répertorie tous les clients configurés qui ne sont pas utilisés pour la sauvegarde et qui n'ont aucun périphérique configuré.
Sélections requises :	aucune
Sélections facultatives :	aucune
Formats pris en charge :	tous les formats
option omnirpt :	`hosts_unused`

Périphériques configurés non utilisés par Data Protector

`Description:`	Répertorie les périphériques de destination configurés non utilisés pour la sauvegarde, la copie d'objet ou la consolidation d'objet.

Sélections requises :	aucune
Sélections facultatives :	aucune
Formats pris en charge :	tous les formats
option omnirpt :	`dev_unused`

Attribution de licences

Description :	Répertorie toutes les licences et le nombre de licences disponibles.
Sélections requises :	aucune
Sélections facultatives :	aucune
Formats pris en charge :	tous les formats
option omnirpt :	`licensing`

Consulter la planification

Description :	Répertorie toutes les spécifications de sauvegarde, de copie d'objet, de consolidation d'objet ou de vérification qui sont planifiées pour démarrer dans le nombre de jours spécifié, jusqu'à un an à l'avance.
Sélections requises :	nombre de jours
Sélections facultatives :	aucune
Formats pris en charge :	tous les formats
option omnirpt :	`lookup_sch`

Rapports de l'IDB

Les rapports de l'IDB fournissent des informations sur la taille de l'IDB.

Taille de l'IDB

Description :	Fournit un tableau contenant des informations sur la base de données de gestion des supports, la base de données catalogue, les fichiers journaux

	archivés, les fichiers de données, les statistiques des répertoires de fichiers binaires du catalogue des détails, SMBF (répertoire `msg`) et l'espace disque insuffisant pour l'IDB.
Sélections requises :	aucune
Sélections facultatives :	aucune
Formats pris en charge :	tous les formats
option omnirpt :	`db_size`

IMPORTANT :
Les colonnes **Utilisé** dans ce rapport indiquent le pourcentage d'éléments utilisés pour chaque partie de l'IDB. Ce pourcentage s'obtient par la division du nombre actuel d'éléments par le nombre maximal d'éléments pour une partie de l'IDB spécifique. Si le nombre d'éléments est illimité, ce chiffre est toujours de 0 %.

Pour savoir si certaines parties de l'IDB manquent d'espace, vous pouvez aussi configurer la notification Espace IDB insuffisant.

Rapports sur les pools et les supports

Les rapports sur les pools et les pools de supports fournissent des informations sur les pools de supports et les supports utilisés.

Liste de supports étendue

Description :	Répertorie tous les supports correspondant aux critères de recherche spécifiés. Pour chaque support, il fournit des informations sur l'ID du support, l'étiquette du support, l'emplacement du support, l'état du support, la protection du support, l'espace utilisé et total (Mo), le dernier accès au support, le pool de support et le type de support, les spécifications de session ayant utilisé le support pour la sauvegarde, la copie d'objet ou la consolidation d'objet, ainsi que le type et le sous-type de session.
Sélections requises :	aucune
Sélections facultatives :	spécification(s) de session, groupe de spécifications de sauvegarde, description, emplacement(s), nom(s) de pool, type de support (DDS, DLT, etc.), état, expiration, période, périphérique(s) de bibliothèque
Formats pris en charge :	tous les formats
option omnirpt :	`media_list_extended`

Liste des supports

Description :	Répertorie tous les supports correspondant aux critères de recherche spécifiés. Pour chaque support, il fournit des informations sur l'ID du support, l'étiquette du support, l'emplacement du support, l'état du support, la protection du support, l'espace utilisé et total (Mo), le dernier accès au support, le pool de supports et le type de support.
Sélections requises :	aucune
Sélections facultatives :	description, emplacement(s), nom(s) de pool, type de support (DDS, DLT, etc.), état, expiration, période, périphérique(s) de bibliothèque
Formats pris en charge :	tous les formats
option omnirpt :	`media_list`

Liste des pools

Description :	Répertorie tous les pools correspondant aux critères de recherche spécifiés. Pour chaque pool, il fournit des informations sur le nom du pool, la description, le type de support, le nombre total de supports, le nombre de supports complets et avec ajout possible contenant des données protégées, le nombre de supports libres ne contenant pas de données protégées, le nombre de supports en état bon, passable ou médiocre.
Sélections requises :	aucune
Sélections facultatives :	nom(s) de pool, emplacement(s), type de support (DDS, DLT, etc.), périphérique(s) de bibliothèque, période
Formats pris en charge :	tous les formats
option omnirpt :	`pool_list`

Statistiques sur les supports

Description :	Statistiques sur les supports correspondant aux critères de recherche. Les informations suivantes sont fournies : nombre de supports ; nombre de supports scratchés ; nombre de supports protégés et en état bon, passable et médiocre ; nombre de supports avec ajout possible ; espace total, utilisé et libre sur le support.
Sélections requises :	aucune
Sélections	description, emplacement(s), nom(s) de pool, type de support (DDS, DLT,

facultatives :	etc.), condition, état, expiration, période, périphérique(s) de bibliothèque
Formats pris en charge :	tous les formats
option omnirpt :	`media_statistics`

Rapports de spécification de session

Les rapports de spécification de session fournissent des informations sur les sauvegardes, la copie d'objet, la consolidation d'objet ou la vérification d'objet, comme la taille moyenne des objets sauvegarde, le planning des sessions, les systèmes de fichiers non configurés pour la sauvegarde, etc.

Taille moyenne des objets sauvegarde

Description :	Affiche la taille moyenne d'un objet dans la spécification de sauvegarde indiquée. Affiche la taille de la sauvegarde complète et incrémentale de l'objet. La caractéristique VADP adoptée par Data Protector 8.14 offre des rapports améliorés pour les machines virtuelles. Les machines virtuelles VMware sont représentées comme des clients Data Protector, appelés clients VADP. Le nouveau format de nom d'objet pour les clients VADP est le suivant : `<hostname>:/<vCenter>/<path>/<vmname> [<UUID>]` Ici, `<hostname>` est le nom DNS de la machine virtuelle hébergée. Si le nom DNS est inconnu, l'adresse IP ou le nom VM est utilisé.
Sélections requises :	aucune
Sélections facultatives :	spécification(s) de sauvegarde, groupe de spécifications de sauvegarde, nombre de jours (à partir du début du rapport, en ordre inverse)
Formats pris en charge :	tous les formats
option omnirpt :	`obj_avesize`

Systèmes de fichiers non configurés pour la sauvegarde

Description :	Répertorie tous les disques (systèmes de fichiers) qui ne sont configurés dans aucune des spécifications de sauvegarde sélectionnées.
Sélections requises :	aucune
Sélections facultatives :	spécification(s) de sauvegarde, groupe de spécifications de sauvegarde

Formats pris en charge :	tous les formats
option omnirpt :	`fs_not_conf`

Dernière sauvegarde de l'objet

Description :	Répertorie tous les objets dans l'IDB. Pour chaque objet, il affiche l'heure de la dernière sauvegarde complète et de la dernière sauvegarde incrémentale, l'heure de la dernière copie d'objet complète et de la dernière copie d'objet incrémentale, et l'heure de la dernière consolidation d'objet. La caractéristique VADP adoptée par Data Protector 8.14 offre des rapports améliorés pour les machines virtuelles. Les machines virtuelles VMware sont représentées comme des clients Data Protector, appelés clients VADP. Le nouveau format de nom d'objet pour les clients VADP est le suivant : `<hostname>:/<vCenter>/<path>/<vmname> [<UUID>]` Ici, `<hostname>` est le nom DNS de la machine virtuelle hébergée. Si le nom DNS est inconnu, l'adresse IP ou le nom VM est utilisé. Vous pouvez restreindre les objets répertoriés à l'aide de filtres de spécification de sauvegarde et/ou d'un filtre d'heure de création de l'objet (voir `Optional Selections`). Cependant, prenez les éléments suivants en compte : • Les objets du type Système de fichiers (objets système de fichiers) qui ne correspondent pas à la condition dans le filtre d'heure de création de l'objet sont quand même répertoriés. Cependant, dans ce cas, leurs champs d'heure de création de l'objet restent vides. • Si vous supprimez certains objets système de fichiers d'une spécification de sauvegarde, ceux-ci ne seront pas inclus dans le rapport même si les objets existent dans l'IDB. Les points ci-dessus ne s'appliquent pas aux objets du type Bar (objets d'intégration).
Sélections requises :	aucune
Sélections facultatives :	spécification(s) de sauvegarde, groupe de spécifications de sauvegarde, nombre de jours (à partir du début du rapport, en ordre inverse)
Formats pris en charge :	tous les formats
option omnirpt :	`obj_lastbackup`

Objets sans sauvegarde

Description :	Répertorie tous les objets faisant partie d'une spécification de sauvegarde et qui n'ont pas de sauvegarde valide (sauvegarde réussie avec succès, protection n'ayant pas encore expiré). Ce rapport n'est pas disponible pour les spécifications de sauvegarde pour les intégrations.
Sélections requises :	aucune
Sélections facultatives :	spécification(s) de sauvegarde, groupe de spécifications de sauvegarde, nombre de jours (à partir du début du rapport, en ordre inverse)
Formats pris en charge :	tous les formats
option omnirpt :	`obj_nobackup`

Informations sur les spécifications de session

Description :	Affiche des informations sur toutes les spécifications de sauvegarde, de copie d'objet, de consolidation d'objet et de vérification d'objet sélectionnées, comme le type (par exemple IDB, MSESE, E2010), le type de session, le nom de spécification de session, le groupe, le propriétaire, les commandes pré-exécution et post-exécution.
Sélections requises :	aucune
Sélections facultatives :	spécification(s) de session, groupe de spécifications de sauvegarde
Formats pris en charge :	tous les formats
option omnirpt :	`dl_info`

Planification des spécifications de session

Description :	Répertorie l'heure de début suivante pour chaque spécification de sauvegarde, de copie d'objet, de consolidation d'objet et de vérification d'objet spécifiée, jusqu'à un an à l'avance.
Sélections requises :	aucune
Sélections facultatives :	spécification(s) de session, groupe de spécifications de sauvegarde
Formats pris en charge :	tous les formats
option omnirpt :	`dl_sched`

Arborescences des spécifications de sauvegarde

Description :	Répertorie toutes les arborescences dans la spécification de sauvegarde spécifiée. Indique également les noms des lecteurs et le nom d'une arborescence. La caractéristique VADP adoptée par Data Protector 8.14 offre des rapports améliorés pour les machines virtuelles. Les machines virtuelles VMware sont représentées comme des clients Data Protector, appelés clients VADP. Le rapport affiche tous les noms VM des objets VMware.
Sélections requises :	aucune
Sélections facultatives :	spécification(s) de sauvegarde, groupe de spécifications de sauvegarde
Formats pris en charge :	tous les formats
option omnirpt :	dl_trees

Rapports de sessions durant la période

Les Rapports Sessions durant la période fournissent des informations sur les sessions de sauvegarde, de copie d'objet, de consolidation d'objet ou de vérification d'objet exécutées durant une période spécifique.

Statistiques sur le client

Description :	Répertorie les clients et leurs statistiques d'état de sauvegarde. Seuls les clients correspondant aux critères de recherche sont répertoriés. La caractéristique VADP adoptée par Data Protector 8.14 offre des rapports améliorés pour les machines virtuelles. Les machines virtuelles VMware sont représentées comme des clients Data Protector, appelés clients VADP, où le nom VM est le nom du client.
Sélections requises :	période
Sélections facultatives :	spécification(s) de sauvegarde, groupe de spécifications de sauvegarde, nom(s) d'hôte
Formats pris en charge :	tous les formats
option omnirpt :	`host_statistics`

Flux de périphérique

Description :	Présente sous forme graphique l'utilisation de chaque périphérique. Un graphique des sessions de sauvegarde, de copie d'objet et de consolidation d'objet correspondant aux critères de recherche est affiché. Si vous définissez l'option globale `RptShowPhysicalDeviceInDeviceFlowReport` sur 1, les périphériques physiques identiques (présentés selon leurs noms de verrouillage ou numéros de série) sont regroupés. Si aucun nom de verrouillage ou numéro de série n'est indiqué, le nom logique est affiché.
Sélections requises :	période
Sélections facultatives :	spécification(s) de session, groupe de spécifications de sauvegarde
Formats pris en charge :	HTML
option omnirpt :	`device_flow`

Rapport détaillé sur les supports utilisés

Description :	Fournit des informations détaillées sur les supports de destination ayant été utilisés par des sessions de sauvegarde, de copie d'objet et de consolidation d'objet durant la période spécifique, ainsi que le type et le sous-type de session.
Sélections requises :	période
Sélections facultatives :	spécification(s) de session, groupe de spécifications de sauvegarde
Formats pris en charge :	tous les formats
option omnirpt :	`used_media_extended`

Liste des sessions

Description :	Répertorie toutes les sessions et leurs statistiques durant la période spécifiée.
Sélections requises :	période
Sélections facultatives :	spécification(s) de session, groupe de spécifications de sauvegarde
Formats pris en charge :	tous les formats
option omnirpt :	`list_sessions`

Copies d'objets

Description :	Affiche le nombre de copies valides de versions d'objets durant la période spécifiée. Le nombre de copies inclut la version d'origine de l'objet. Les machines virtuelles VMware sont représentées comme des clients Data Protector, appelés clients VADP. Le nouveau format de nom d'objet pour les clients VADP est le suivant : `<hostname>:/<vCenter>/<path>/<vmname> [<UUID>]` Ici, `<hostname>` est le nom DNS de la machine virtuelle hébergée. Si le nom DNS est inconnu, l'adresse IP ou le nom VM est utilisé.
Sélections requises :	période
Sélections facultatives :	spécification(s) de session, groupe de spécifications de sauvegarde, nombre de copies
Formats pris en charge :	tous les formats
option omnirpt :	`obj_copies`

Rapport sur les supports utilisés

Description :	Répertorie les supports de destination ayant été utilisés durant les sessions de sauvegarde, de copie d'objet et de consolidation d'objet durant la période spécifiée, ainsi que les statistiques connexes.
Sélections requises :	période
Sélections facultatives :	spécification(s) de session, groupe de spécifications de sauvegarde
Formats pris en charge :	tous les formats
option omnirpt :	`used_media`

Erreurs de session

Description :	Affiche une liste de messages d'erreur qui se sont produits durant une session de sauvegarde, de copie d'objet, de consolidation d'objet ou de vérification d'objet. Les messages sont regroupés par client.
Sélections requises :	période
Sélections facultatives :	spécification(s) de sauvegarde, groupe de spécifications de sauvegarde, nom(s) d'hôte, niveau de message

Formats pris en charge :	tous les formats
option omnirpt :	`session_errors`

Flux de session

Description :	Présente sous forme graphique la durée de chaque session pendant la période spécifiée. Un graphique des sessions de sauvegarde, de copie d'objet, de consolidation d'objet et de vérification d'objet correspondant aux critères de recherche est affiché. Les couleurs du graphique représentent l'état global suivant des sessions : • Rouge : La session a échoué ou a été annulée. • Vert : La session s'est terminée avec succès ou avec des erreurs. • Jaune : La session terminée avec erreurs. • Bleu : La session est en file d'attente ou une demande de montage est émise.
Sélections requises :	période
Sélections facultatives :	spécification(s) de session, groupe de spécifications de sauvegarde
Formats pris en charge :	HTML
option omnirpt :	`session_flow`

Statistiques de session

Description :	Affiche les statistiques sur l'état de la sauvegarde, la copie d'objet ou la consolidation d'objet durant la période sélectionnée.
Sélections requises :	période
Sélections facultatives :	spécification(s) de session, groupe de spécifications de sauvegarde
Formats pris en charge :	tous les formats
option omnirpt :	`session_statistics`

Rapports de session unique

Les rapports de session unique fournissent des informations détaillées sur une session spécifique.

Périphériques de session

Description :	Fournit des informations sur tous les périphériques de destination utilisés durant la session sélectionnée.
Sélections requises :	ID de session
Sélections facultatives :	aucune
Formats pris en charge :	tous les formats
option omnirpt :	`session_devices`

Supports de session

Description :	Fournit des informations sur tous les supports de destination utilisés durant la session sélectionnée.
Sélections requises :	ID de session
Sélections facultatives :	aucune
Formats pris en charge :	tous les formats
option omnirpt :	`session_media`

Copies d'objets de la session

Description :	Affiche le nombre de copies valides dans une session de sauvegarde, de copie d'objet ou de consolidation d'objet. La caractéristique VADP adoptée par Data Protector 8.14 offre des rapports améliorés pour les machines virtuelles. Les machines virtuelles VMware sont représentées comme des clients Data Protector, appelés clients VADP. Le nouveau format de nom d'objet pour les clients VADP est le suivant : `<hostname>:/<vCenter>/<path>/<vmname> [<UUID>]` Ici, `<hostname>` est le nom DNS de la machine virtuelle hébergée. Si le nom DNS est inconnu, l'adresse IP ou le nom VM est utilisé.
Sélections requises :	ID de session
Sélections facultatives :	aucune

Formats pris en charge :	tous les formats
option omnirpt :	`session_objcopies`

Objets de session

Description :	Répertorie tous les objets sauvegarde, de copie d'objet ou de consolidation d'objet, ainsi que leurs statistiques, qui ont fait partie d'une session sélectionnée. La caractéristique VADP adoptée par Data Protector 8.14 offre des rapports améliorés pour les machines virtuelles. Les machines virtuelles VMware sont représentées comme des clients Data Protector, appelés clients VADP. Le rapport Objets de session affiche le nom et le chemin d'accès VM.
Sélections requises :	ID de session
Sélections facultatives :	aucune
Formats pris en charge :	tous les formats
option omnirpt :	`session_objects`

Session par client

Description :	Fournit des informations sur chaque client qui a fait partie de la session de sauvegarde sélectionnée. Avec l'option **Générer plusieurs rapports**, ce rapport peut être divisé en rapports plus petits, avec un rapport pour chaque client. Les machines virtuelles VMware sont représentées comme des clients Data Protector, appelés clients VADP. Le nouveau format de nom d'objet pour les clients VADP est le suivant : `<hostname>:/<vCenter>/<path>/<vmname> [<UUID>]` Ici, `<hostname>` est le nom DNS de la machine virtuelle hébergée. Si le nom DNS est inconnu, l'adresse IP ou le nom VM est utilisé.
Sélections requises :	ID de session
Sélections facultatives :	niveau de message
Formats pris en charge :	tous les formats
option omnirpt :	`session_hosts`

Session unique

Description :	Affiche toutes les informations utiles sur une session de sauvegarde, de copie d'objet ou de consolidation d'objet Data Protector unique.
Sélections requises :	ID de session
Sélections facultatives :	niveau de message
Formats pris en charge :	tous les formats
option omnirpt :	`single_session`

Méthodes d'envoi de rapports

Vous pouvez choisir parmi plusieurs méthodes d'envoi lorsque vous configurez un rapport ou un groupe de rapports.

Méthode d'envoi de message de diffusion

La méthode d'envoi de message de diffusion permet d'envoyer un message de diffusion avec la sortie du rapport vers des systèmes spécifiés.

Les messages de diffusion peuvent être envoyés (seulement vers des systèmes Windows) en spécifiant le système de destination. Les messages de diffusion sont limités à 1000 caractères ; le format court est donc conseillé.

Méthode d'envoi d'e-mail

Vous pouvez envoyer un e-mail contenant les informations du rapport à des destinataires spécifiés. Indiquez l'adresse e-mail complète du destinataire.

IMPORTANT :
En raison des fonctions de sécurité de Microsoft Outlook, l'utilisation de la méthode d'envoi d'e-mail peut provoquer un arrêt de réponse du service CRS. Pour plus d'informations, reportez-vous à *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*. Sinon, utilisez la méthode d'envoi d'e-mail SMTP.

REMARQUE :
Si Microsoft Exchange Server 2007 est installé sur le Gestionnaire de cellule Data Protector, la méthode d'envoi de rapports par e-mail ne fonctionne pas. Dans ce cas, utilisez la méthode d'envoi e-mail (SMTP).

Sur les systèmes Windows

Pour envoyer un rapport par e-mail à partir d'un système Windows, vous devez disposer d'un profil de messagerie. Vous pouvez utiliser un profil de messagerie existant ou en créer un nouveau, nommé `OmniBack`.

Pour utiliser un profil de messagerie existant, ajoutez la ligne suivante au fichier : Data Protector `omnirc`

`OB2_MAPIPROFILE=`*`existing_MAPI_profile_name`*

L'affichage de rapports électroniques au format HTML sous Windows dépend des paramètres du client de messagerie. Un grand nombre de clients de messagerie affichent les rapports au format ASCII (texte brut). Pour vous assurer que les rapports s'affichent bien au format HTML, ouvrez-les dans un navigateur Web.

Sur les systèmes UNIX

Le sous-système d'e-mail doit être configuré et exécuté sur un système UNIX. Aucune configuration supplémentaire n'est requise.

En raison des limites de ce système d'exploitation, les caractères internationaux présents dans les rapports électroniques localisés peuvent ne pas s'afficher correctement sur les systèmes UNIX dans le cas de transmissions entre des systèmes n'utilisant pas les mêmes paramètres régionaux.

Méthode d'envoi d'e-mail (SMTP)

Vous pouvez envoyer un e-mail contenant les informations du rapport à des destinataires spécifiés à l'aide du protocole SMTP. Indiquez l'adresse e-mail complète du destinataire.

Il s'agit de la méthode d'envoi d'e-mail recommandée.

Par défaut, l'adresse du serveur SMTP utilisé pour l'envoi des rapports correspond à l'adresse IP du Gestionnaire de cellule. Pour modifier l'adresse, éditez l'option globale `SMTPServer`. Le serveur SMTP doit être accessible à partir du système du Gestionnaire de cellule, mais peut ne pas appartenir à la cellule Data Protector.

Sur les systèmes Windows

Pour plus d'informations sur la configuration du serveur Microsoft Exchange existant pour prendre en charge le protocole SMTP, reportez-vous à la documentation de Microsoft Exchange Server.

L'affichage de rapports électroniques au format HTML sous Windows dépend des paramètres du client de messagerie. Un grand nombre de clients de messagerie affichent les rapports au format ASCII (texte brut). Pour vous assurer que les rapports s'affichent bien, ouvrez-les dans un navigateur Web.

Sur les systèmes UNIX

En raison des limites du système d'exploitation, les caractères internationaux présents dans les rapports électroniques localisés peuvent ne pas s'afficher correctement sous UNIX en cas de transmission entre des systèmes n'utilisant pas les mêmes paramètres régionaux.

Méthode d'envoi externe

La méthode d'envoi de script externe permet d'effectuer la sortie du rapport sur votre propre script. Le script reçoit la sortie comme entrée standard (STDIN). Le format recommandé pour le traitement du script est le format tab.

Le script, qui se trouve sur le système du Gestionnaire de cellule, doit être enregistré dans le répertoire `/opt/omni/lbin` (systèmes HP-UX) ou *`répertoire_Data_Protector`*`\bin` (systèmes Windows). N'indiquez que le nom du script, pas la totalité du chemin d'accès.

Notez que seules les extensions `.bat`, `.exe` et `.cmd` sont prises en charge pour les scripts externes sur les systèmes Windows. Pour exécuter un script avec une extension non prise en charge (par exemple, `.vbs`), créez un fichier de commandes qui démarre le script. Configurez ensuite Data Protector pour exécuter le fichier de commandes en tant que script externe, qui lance à son tour le script avec l'extension non prise en charge.

Vous pouvez également utiliser cette méthode d'envoi pour réaliser une éjection planifiée des supports spécifiés.

Méthode d'envoi Journaliser dans un fichier

La méthode d'envoi Journaliser dans un fichier permet d'envoyer un fichier contenant la sortie du rapport.

Le fichier est envoyé au système du Gestionnaire de cellule. Vous devez préciser le nom du fichier vers lequel vous souhaitez envoyer le rapport. Le fichier sera écrasé s'il existe.

Méthode d'envoi SNMP

La méthode d'envoi par interruption SNMP permet d'envoyer un rapport sous la forme d'une interruption SNMP. L'interruption SNMP peut être ensuite traitée par des applications utilisant les interruptions SNMP.

> **REMARQUE :**
> Vous devez réserver la méthode d'envoi SNMP aux rapports dont la taille maximum n'excède pas celle de l'interruption SNMP configurée. Sinon, le rapport est fragmenté.

Sur les systèmes Windows

Les interruptions SNMP sont envoyées aux systèmes configurés dans la configuration d'interruptions SNMP Windows. Vous devez configurer les interruptions SNMP Windows pour pouvoir utiliser la méthode d'envoi SNMP dans le Gestionnaire de cellule.

Sur les systèmes UNIX

Sur un Gestionnaire de cellule UNIX, les interruptions SNMP sont envoyées aux systèmes configurés dans le rapport.

Configuration de groupes de rapports à l'aide de l'interface graphique utilisateur HPE Data Protector

Vous pouvez exécuter les rapports Data Protector individuellement (de manière interactive), ou les rassembler dans un groupe et ainsi lancer le groupe de rapports. Vous pouvez ajouter des rapports individuels à un groupe de rapports déjà configuré. Les rapports sur la demande de montage et sur les erreurs de périphérique ne peuvent être utilisés que dans un groupe de rapports, ils ne sont pas disponibles en tant que rapports interactifs.

Via l'interface graphique utilisateur Data Protector, un groupe de rapports vous permet de :

- Lancer tous les rapports en une seule fois (de manière interactive).
- Planifier le groupe pour lancer les rapports à un moment déterminé.
- Lancer le groupe sur déclenchement par notification.

Pour afficher les paramètres d'entrée (sélections) dans un rapport, activez l'option **Afficher critères de sélection dans le rapport** dans l'assistant de rapport. Cette option n'est pas disponible pour les rapports n'ayant aucun paramètre d'entrée obligatoire ou facultatif (sélections). Les résultats du rapport ne contiennent que les paramètres obligatoires et facultatifs dont les valeurs par défaut sont modifiées.

Conditions préalables

- Vous devez faire partie du groupe d'utilisateurs `admin`ou disposer des droits d'utilisateur de rapports et notifications.
- L'utilisateur Data Protector sous le compte duquel le service CRS est exécuté ne doit pas être supprimé. Cet utilisateur est configuré par défaut lors de l'installation. Sur un Gestionnaire de cellule Windows, il s'agit de l'utilisateur sous le compte duquel l'installation a été effectuée. Sur un Gestionnaire de cellule UNIX, il s'agit de l'utilisateur `root`du Gestionnaire de cellule.

Etapes de la configuration

Configuration d'un groupe de rapports

Procédure

1. Dans la liste de contexte, sélectionnez **Création de rapports**.
2. Cliquez avec le bouton droit sur **Rapports**, puis choisissez **Ajouter groupe de rapports** pour lancer l'assistant.
3. Nommez le groupe de rapports et cliquez sur **Suivant**.
4. Cliquez sur **Terminer** pour ajouter le groupe de rapports et quitter l'assistant. Vous pouvez maintenant exécuter si vous le souhaitez les actions suivantes :
   - Planifier le groupe de rapports : cliquez avec le bouton droit sur le groupe de rapports et cliquez sur **Modifier la planification**. La page du planificateur s'affiche. Pour plus d'informations sur la création et la modification de planifications dans Data Protector à l'aide du planificateur, voir *Planificateur, Page 110*.

- Ajouter des rapports au groupe de rapports : cliquez avec le bouton droit sur le groupe de rapports et cliquez sur **Ajouter rapport**. Suivez les instructions de l'assistant d'ajout de rapport.

> **CONSEIL :**
> Pour déclencher un groupe de rapports par une notification, configurez un groupe de rapports, puis la notification avec la méthode d'envoi Utiliser le groupe de rapports.

Ajout d'un rapport dans un groupe de rapports

Procédure

1. Dans le contexte de génération de rapports, développez **Rapports**, cliquez avec le bouton droit de la souris sur un groupe de rapports, puis sélectionnez **Ajouter rapport** pour lancer l'assistant. En cas de configuration d'un rapport juste après celle du groupe de rapports, ignorez cette étape.
2. Dans la liste affichée dans la zone de résultats, sélectionnez un type de rapport.
3. Nommez votre rapport dans la zone de texte Nom et sélectionnez un rapport dans la liste déroulante Type. Cliquez sur **Suivant**.
4. Les options disponibles dans l'assistant dépendent du rapport sélectionné. Par exemple, toutes les options de l'assistant disponibles pour le rapport sur la taille de l'IDB ne sont pas disponibles pour le rapport sur la liste des supports. Cliquez sur **Suivant** autant de fois que cela est nécessaire pour atteindre la dernière page de l'assistant.
5. Dans la liste déroulante de la méthode d'envoi, sélectionnez la méthode d'envoi du rapport, puis indiquez le destinataire du rapport dans la zone de texte de l'adresse e-mail. Dans la liste déroulante Format, sélectionnez le format du rapport. Cliquez sur **Ajouter** pour ajouter le destinataire au groupe de destinataires configurés.

   Répétez cette étape pour tous les destinataires.
6. Cliquez sur **Terminer** pour ajouter le groupe de rapports et quitter l'assistant.

Répétez cette procédure pour tous les rapports à ajouter à un groupe de rapports.

Exécution de groupes de rapports à l'aide de l'interface graphique HPE Data Protector

Vous pouvez exécuter simultanément tous les rapports d'un groupe.

Conditions préalables

- Vous devez faire partie du groupe d'utilisateurs Admin ou disposer des droits d'utilisateur de rapports et notifications.
- L'utilisateur Data Protector sous le compte duquel le service CRS est exécuté ne doit pas être supprimé. Cet utilisateur est configuré par défaut lors de l'installation. Sur un Gestionnaire de cellule Windows, il s'agit de l'utilisateur sous le compte duquel l'installation a été effectuée. Sur un Gestionnaire de cellule UNIX, il s'agit de l'utilisateur `root`du Gestionnaire de cellule.

Procédure

1. Dans la liste de contexte, sélectionnez **Création de rapports**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le groupe de rapports que vous souhaitez lancer, puis cliquez sur **Démarrer**.
3. Cliquez sur **Oui** pour confirmer.

Exécution de rapports individuels à l'aide de l'interface graphique utilisateur HPE Data Protector

Vous pouvez exécuter des rapports individuels de manière interactive, ou les rassembler dans un groupe et ainsi exécuter simultanément tous les rapports d'un groupe.

Les rapports sur la demande de montage et sur les erreurs de périphérique ne peuvent être utilisés que dans un groupe de rapports et ne sont pas disponibles en tant que rapports interactifs.

Conditions préalables

- Vous devez faire partie du groupe d'utilisateurs Admin ou disposer des droits d'utilisateur de rapports et notifications.
- L'utilisateur Data Protector sous le compte duquel le service CRS est exécuté ne doit pas être supprimé. Cet utilisateur est configuré par défaut lors de l'installation. Sur un Gestionnaire de cellule Windows, il s'agit de l'utilisateur sous le compte duquel l'installation a été effectuée. Sur un Gestionnaire de cellule UNIX, il s'agit de l'utilisateur `root`du Gestionnaire de cellule.

Procédure

1. Dans la liste de contexte, sélectionnez **Création de rapports**.
2. Cliquez sur l'onglet **Tâches** sous la fenêtre de navigation.
3. Dans la fenêtre de navigation, recherchez le type de rapport souhaité et sélectionnez un rapport pour ouvrir l'assistant.
4. Les options disponibles dans l'assistant dépendent du rapport sélectionné. Par exemple, toutes les options de l'assistant disponibles pour le rapport sur la taille de l'IDB ne sont pas disponibles pour le rapport sur la liste des supports. Cliquez sur **Suivant** autant de fois que cela est nécessaire pour atteindre la dernière page de l'assistant.
5. Cliquez alors sur **Terminer** pour afficher les résultats du rapport.

Exécution de rapports et de groupes de rapports à l'aide de l'interface de ligne de commande HPE Data Protector

Vous pouvez générer des rapports Data Protector à l'aide de l'interface de ligne de commande (CLI). Celle-ci vous permet d'intégrer des rapports Data Protector dans d'autres scripts que vous utilisez. Vous pouvez générer des rapports individuels, lancer des groupes de rapports et définir des formats et des méthodes d'envoi de rapports.

Conditions préalables

- Vous devez faire partie du groupe d'utilisateurs Admin ou disposer des droits d'utilisateur de rapports et notifications.
- L'utilisateur Data Protector sous le compte duquel le service CRS est exécuté ne doit pas être supprimé. Cet utilisateur est configuré par défaut lors de l'installation. Sur un Gestionnaire de cellule Windows, il s'agit de l'utilisateur sous le compte duquel l'installation a été effectuée. Sur un Gestionnaire de cellule UNIX, il s'agit de l'utilisateur `root` du Gestionnaire de cellule.

Procédure

1. Utilisez la commande `omnirpt` pour générer les rapports. Pour obtenir la description détaillée de la commande, consultez la page `omnirpt` du manuel *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Création d'un profil de messagerie

Pour envoyer un rapport ou une notification par e-mail à partir d'un système Windows, vous devez disposer d'un profil de messagerie. Pour créer un profil de messagerie, nommé `OmniBack`, sur un système Windows avec Microsoft Outlook 2002, suivez la procédure ci-dessous.

> **IMPORTANT :**
> En raison des fonctions de sécurité de Microsoft Outlook, l'utilisation de la méthode d'envoi d'e-mail peut provoquer un arrêt de réponse du service CRS. Pour plus d'informations, reportez-vous à *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*. De manière alternative, utilisez la méthode d'envoi `e-mail (SMTP)`.

Procédure

1. Dans le Panneau de configuration de Windows, double-cliquez sur l'icône **Courrier**.
2. Dans la boîte de dialogue Configuration de la messagerie Outlook, cliquez sur **Afficher les profils**
3. Dans la boîte de dialogue Courrier, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue Nouveau profil, entrez `OmniBack` dans la zone de texte Nom du profil, puis cliquez sur **OK** pour lancer l'assistant Comptes de messagerie.
5. Sélectionnez **Ajouter un nouveau compte de messagerie** et cliquez sur **Suivant**.
6. Dans la page Type de serveur, sélectionnez **Microsoft Exchange Server** et cliquez sur **Suivant**.
7. Dans la page Paramètres d'Exchange Server, entrez le nom du système Microsoft Exchange Server local ainsi que votre nom d'utilisateur. Cliquez sur **Suivant**.
8. Cliquez sur **Terminer** pour quitter l'assistant.

Configuration d'interruptions SNMP Windows

Sur un Gestionnaire de cellule Windows, les interruptions SNMP sont envoyées aux systèmes définis dans la configuration d'interruptions SNMP Windows. Sous Windows, pour envoyer une notification ou

un rapport en utilisant la méthode d'envoi SNMP, vous devez configurer les interruptions SNMP.

Sur un Gestionnaire de cellule UNIX, les interruptions SNMP sont envoyées aux systèmes configurés dans la notification ou le rapport. Aucune configuration supplémentaire n'est requise.

Procédure

1. Dans le répertoire *répertoire_Data_Protector*\bin, appelez la commande omnisnmp.

   L'entrée Data Protector appropriée est créée dans le registre système sous CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents.
2. **Windows XP, Windows Server 2003 :**
   a. Dans le Panneau de configuration, sélectionnez **Connexions réseau**.
   b. Dans le menu Avancé, cliquez sur **Composants de gestion réseau optionnels** pour démarrer l'assistant.
   c. Sélectionnez **Outils de gestion et d'analyse**, puis cliquez sur **Suivant**.
   d. Suivez les indications de l'assistant pour installer ces outils.

   Windows 7, Windows 8 :
   a. Dans le Panneau de configuration, sélectionnez **Programmes et fonctionnalités**.
   b. Sélectionnez **Activer ou désactiver des fonctionnalités Windows**.
   c. Sélectionnez **Protocole SNMP (Simple Network Management Protocol)** et cliquez sur **OK**.

   Windows Server 2008, Windows Server 2012 :
   a. Dans le menu Démarrer, cliquez avec le bouton droit de la souris sur **Ordinateur** et sélectionnez **Gérer**.
   b. Sélectionnez **Fonctionnalités** et cliquez sur **Ajouter des fonctionnalités**.
   c. Dans l'arborescence Fonctionnalités, sélectionnez **Services SNMP** puis **Service SNMP**.
   d. Cliquez sur **Suivant** puis sur **Installer**.
3. Ouvrez le menu **Panneau de configuration**, **Outils d'administration**, **Services**.
4. Cliquez avec le bouton droit de la souris sur **Service SNMP** et sélectionnez **Propriétés**.
   a. Sélectionnez l'onglet **Interruptions**. Saisissez public dans la zone de texte Nom de communauté, ainsi que le nom d'hôte du dans la zone de texte Destinations des interruptions.
   b. Sélectionnez l'onglet **Sécurité**. Sous Noms de communauté acceptés, sélectionnez la communauté public, cliquez sur **Modifier** et spécifiez les droits de communauté READ CREATE.

      Si vous sélectionnez **Accepter ci-dessous les paquets SNMP depuis ces hôtes** et que l'authentification échoue, utilisez alors l'adresse IP à la place du nom d'hôte dans la zone de texte Destinations des interruptions.
   c. Confirmez vos modifications.
5. Invoquez omnisnmp.

À propos des notifications

Data Protector permet d'envoyer des notifications à partir du Gestionnaire de cellule lorsque des événements spécifiques se produisent. Par exemple, lorsqu'une session de sauvegarde, de copie d'objet, de consolidation d'objet ou de vérification d'objet est terminée, vous pouvez envoyer un e-mail avec l'état de la session.

Vous pouvez définir une notification de sorte qu'elle déclenche un rapport.

Vous pouvez configurer des notifications à l'aide de l'interface Data Protector ou de tout navigateur Web supportant Java.

Les paramètres d'entrée vous permettent de personnaliser les notifications. Vous pouvez effectuer des sélections multiples avec certains paramètres d'entrée. Tous les autres paramètres d'entrée dépendent du type de la notification. Selon la méthode d'envoi, le destinataire peut être :

- un système
- une adresse e-mail
- une interruption SNMP
- un script
- un fichier
- un groupe de rapports configuré
- le journal d'événements Data Protector

Par défaut, les notifications sont configurées avec des valeurs par défaut et sont envoyées au journal d'événements Data Protector. Pour envoyer des notifications supplémentaires avec d'autres méthodes d'envoi et/ou d'autres paramètres d'entrée, vous devez modifier les valeurs de configuration.

Pour avoir accès à la fonction de notification de Data Protector. Vous devez faire partie du groupe d'utilisateurs `admin` ou disposer des droits d'utilisateur de **rapports et notifications**.

Types de notification - Evénements déclenchant des notifications

Il existe deux types principaux de notifications.

- Les notifications déclenchées lorsqu'un événement se produit
- Les notifications planifiées et démarrées par le mécanisme de maintenance et de vérification de Data Protector

Alarme

Nom événement/notification :	Alarme
Ce qui déclenche la notification :	Conditions internes Data Protector critiques, comme la mise à niveau de la copie automatisée des supports, la fin de la mise à niveau de la partie

	centrale, la fin de la mise à niveau de la partie contenant les détails, la fin de la purge, l'abandon de session, la mise à jour des Agents de disque durant la mise à niveau de la partie centrale, etc.
Niveau du message par défaut :	Avertissement
Message affiché :	Alarme : *`Alarm_message`*

Certificats expirés

Nom événement/notification :	ExpiredCertificates
Ce qui déclenche la notification :	Le certificat stocké dans le répertoire de certificats du Gestionnaire de cellule a expiré ou n'est pas encore valide. Le répertoire de certificats du Gestionnaire de cellule stocke tous les certificats clients pour une communication contrôlée de manière sécurisée.
Niveau du message par défaut :	Avertissement
Message affiché :	Le certificat *nom_certificat* a expiré ou n'est pas encore valable.

Échec de la session Démarrer Csa

Nom événement/notification :	CsaStartSessionFailed
Ce qui déclenche la notification :	La session de sauvegarde qui se termine avec le message d'erreur : `Could not start a new backup session.`
Niveau du message par défaut :	Majeur
Message affiché :	Echec de CsaStartSession pour la liste de données *datalist_name*.

Erreur de périphérique

Nom événement/notification :	DeviceError
Ce qui déclenche la notification :	Une erreur sur le périphérique **Périphérique** (par défaut : `<Any>`).
Niveau du message par défaut :	Critique

Message affiché :	Une erreur s'est produite sur le périphérique *Device*.

Fin de session

Nom événement/notification :	EndofSession
Ce qui déclenche la notification :	Une session de sauvegarde, de copie, de consolidation ou de vérification d'objets spécifiée dans la spécification de session **Spécification de session** (par défaut : <Any>) se terminant avec le message **Etat de la session** (par défaut : Completed with errors).
Niveau du message par défaut :	Avertissement
Messages affichés :	Session de sauvegarde *session_ID* de la spécification de session *backup_specification*, groupe de spécification de sauvegarde *group* terminée avec l'état global *session_overall_status;* *session_type* Session *session_ID* de la spécification de session *session_spec*, terminée avec l'état global *session_status*.

Occupation disque de la bibliothèque de fichiers

Nom événement/notification :	FileLibraryDiskUsage
Ce qui déclenche la notification :	Un manque d'espace disque libre pour la bibliothèque de fichiers **Nom de la bibliothèque de fichiers** (par défaut : All).
Niveau du message par défaut :	Avertissement
Message affiché :	Le *File Library Device* manque d'espace disque dans le répertoire *File Library Path*.

Échec de l'auto-test

Nom événement/notification :	HealthCheckFailed
Ce qui déclenche la notification :	Une valeur non nulle retournée par la commande omnihealthcheck. La commande renvoie zéro si les éléments suivants sont vrais : • Les services Data Protector (CRS, MMD, hpdp-idb, hpdp-idb-cp, hpdp-as, KMS , omnitrig et omniinet) sont actifs. • La base de données de gestion des supports Data Protector (MMDB)

	est cohérente. • Au moins une sauvegarde de l'IDB existe. Pour plus d'informations sur cette commande, reportez-vous à la page de manuel `omnihealthcheck` ou à la *Guide de référence de l'interface de ligne de commande HPE Data Protector*. Par défaut, Data Protector démarre l'auto-test (qui exécute la commande `omnihealthcheck`) une fois par jour.
Niveau du message par défaut :	Critique
Message affiché :	Message d'auto-test : Echec de *`healthcheck_command`*.

Sauvegarde IDB requise

Nom événement/notification :	IDBBackupNeeded
Ce qui déclenche la notification :	Trop de sauvegardes incrémentales de l'IDB successives ou sauvegarde complète de l'IDB pas assez fréquente.
Niveau du message par défaut :	Avertissement
Message affiché :	Il y a *`n`* sauvegardes incrémentales successives. La dernière sauvegarde de la base de données interne de Data Protector a été effectuée le *`MM/DD/YY hh:mm:ss`*.

Base de données interne altérée

Nom événement/notification :	IDBCorrupted
Ce qui déclenche la notification :	Corruption d'une partie de l'IDB.
Niveau du message par défaut :	Critique
Message affiché :	La partie *`IDB_part`* de la base de données interne de Data Protector est altérée (*`error_message`*). Les valeurs du message d'erreur sont : • `Verification of datafile(s) failed.` • `KeyStore is corrupted.` • `Media and Media in position tables are not consistent.` • `Database is not in consistent state.`

	• `Database schema is not consistent.`

Limites IDB

Nom événement/notification :	IDBLimits
Ce qui déclenche la notification :	Limite atteinte de l'une des parties de MMDB ou CDB.
Niveau du message par défaut :	Majeur
Message affiché :	La partie *`IDB_part`* de la base de données interne de Data Protector a atteint sa limite.

Réorganisation de l'IDB requise

Nom événement/notification :	IDBReorganizationNeeded
Ce qui déclenche la notification :	Une ou plusieurs entités IDB doivent être réorganisées en raison d'une fragmentation ou d'espace perdu.
Niveau du message par défaut :	Avertissement
Message affiché :	Inflation de la table *nom_`of_table`* détectée. Fragmentation de la table *`name_of_table`* dans la colonne *`uuid`* détectée. Fragmentation de l'index *`name_of_index`* détectée.

Peu d'espace dans la base de données interne

Nom événement/notification :	IDBSpaceLow
Ce qui déclenche la notification :	L'un des événements suivants : • L'espace disque disponible maximum est inférieur à la valeur de la **Limite d'espace disque libre IDB [Mo]** (par défaut : `300 MB`). • La différence entre la taille maximum et la taille actuelle de tous les répertoires DC est inférieure à la valeur **Seuil de limite de taille DCBF [Mo]** (par défaut : `500 MB`). • L'espace disque disponible maximum est inférieur à la valeur de la **Limite d'espace disque libre WAL [Mo]** (par défaut : `300 MB`). Par défaut, Data Protector vérifie la condition d'espace disque insuffisant

	de l'IDB une fois par jour.
Niveau du message par défaut :	Majeur
Message affiché :	Mémoire insuffisante de la base de données interne Data Protector.

Avertissement concernant la licence

Nom événement/notification :	LicenseWarning
Ce qui déclenche la notification :	Besoin d'acheter des licences.
Niveau du message par défaut :	Avertissement
Message affiché :	*n* licence(s) doivent être achetée(s) pour la catégorie *name of the license*. Exécutez `omnicc -check_licenses -detail` pour plus d'informations.

La licence arrive à expiration

Nom événement/notification :	LicenseWillExpire
Ce qui déclenche la notification :	La date d'expiration à venir de la licence de Data Protector. La licence expirera dans le nombre de jours spécifié dans **La licence expire dans** (par défaut : `10`).
Niveau du message par défaut :	Avertissement
Message affiché :	La première licence expirera dans *License expires in days* jours.

Logements de bande occupés

Nom événement/notification :	MailSlotsFull
Ce qui déclenche la notification :	Logements de bande du périphérique **Périphérique** occupés (par défaut : `<Any>`).
Niveau du message par défaut :	Avertissement
Message affiché :	Tous les logements de bande de la bibliothèque *Device* sont occupés.

	Retirez-les immédiatement.

Demande de montage

Nom événement/notification :	MountRequest
Ce qui déclenche la notification :	Une demande de montage pour le périphérique **Périphérique** (par défaut : `<Any>`).
Niveau du message par défaut :	Avertissement
Message affiché :	Demande de montage sur le périphérique *`Device`*.

Supports libres insuffisants

Nom événement/notification :	NotEnoughFreeMedia
Ce qui déclenche la notification :	Supports libres insuffisants dans le **Pool de supports**. Notez que si un **Pool de supports** est configuré pour utiliser un **Pool libre**, le **Nombre de supports libres** dans le **Pool de supports** est également pris en compte.
Niveau du message par défaut :	Avertissement
Message affiché :	Le pool de supports *`Media Pool`* contient seulement *`number_of_media`* supports libres.

Erreur de session

Nom événement/notification :	SessionError
Ce qui déclenche la notification :	Une session de sauvegarde, de copie, de consolidation ou de vérification d'objets avec un message du niveau Niveau de message unique (par défaut : `Major`) ou supérieur affiché dans la fenêtre du moniteur.
Niveau du message par défaut :	Majeur
Messages affichés :	La session de sauvegarde *`session_ID`* de la spécification de sauvegarde *`backup_specification`*, groupe de sauvegarde *`group`*, contient des erreurs : *`number_of_errors`*. *`session_type`* la session *`session_ID`* de la spécification de session

	session_spec contient des erreurs : *number_of_errors*.

Début de session

Nom événement/notification :	StartofSession
Ce qui déclenche la notification :	Un démarrage d'une session de sauvegarde, de copie, de consolidation ou de vérification d'objets spécifiée dans la spécification de session **Spécification de session** (par défaut : <Any>).
Niveau du message par défaut :	Normal
Messages affichés :	Session de sauvegarde *session_ID* démarrée pour la spécification de session *backup_specification*, groupe de spécification de sauvegarde *group*. *session_type* session *session_ID* démarrée pour la spécification de session *session_spec*.

Trop de sessions

Nom événement/notification :	TooManySessions
Ce qui déclenche la notification :	Démarrage d'une session lorsque 1 000 sessions sont déjà exécutées simultanément.
Niveau du message par défaut :	Avertissement
Message affiché :	Impossible de démarrer la session, car le nombre maximum de sessions s'exécutant simultanément a été atteint.

Evénements inattendus

Nom événement/notification :	UnexpectedEvents
Ce qui déclenche la notification :	Un nombre anormalement élevé de nouveaux événements dans le journal d'événements Data Protector depuis la dernière vérification. Le nombre dépasse le **Nombre d'événements** (par défaut : 20). Par défaut, Data Protector vérifie la condition une fois par jour.
Niveau du message par défaut :	Avertissement

Message affiché :	Le journal d'événements de Data Protector a augmenté de *number_of events_in_last_day* événements inattendus au cours du jour précédent.

Vérifier l'Agent de support UNIX

Nom événement/notification :	UnixMediaAgentWarning
Ce qui déclenche la notification :	La commande `mrgcfg -check_ma` déclenche cette notification lorsque les périphériques clients utilisent des fichiers de périphérique à rembobinage au lieu de fichiers de périphérique sans rembobinage.
Niveau du message par défaut :	Avertissement
Message affiché :	Des Agents de support, périphériques client ont peut-être été configurés à l'aide de fichiers de périphérique avec rembobinage au lieu de fichiers de périphérique sans rembobinage. Ceci peut causer des problèmes dans les environnements SAN.

Echec de la vérification de l'utilisateur

Nom événement/notification :	UserCheckFailed
Ce qui déclenche la notification :	Une valeur autre que zéro renvoyée par le script/la commande créé(e) par l'utilisateur avec le nom **Chemin commande** situé dans le répertoire des commandes administratives Data Protector par défaut. Par défaut, Data Protector démarre la vérification utilisateur (qui exécute le script) une fois par jour (par défaut : `None`).
Niveau du message par défaut :	Majeur
Message affiché :	Echec de la vérification de l'utilisateur avec le code de sortie *error_ code* :*error_description*.

Méthodes d'envoi de notifications

Vous pouvez choisir entre plusieurs méthodes d'envoi lors de la configuration d'une notification. Par défaut, toutes les notifications sont configurées pour être envoyées au journal d'événements Data Protector. Pour envoyer une notification à l'aide d'une autre méthode d'envoi, vous devez configurer une notification supplémentaire. Les méthodes d'envoi de notifications disponibles sont les suivantes :

Méthode d'envoi de message de diffusion

La méthode d'envoi de message de diffusion vous permet d'envoyer un message de diffusion avec la sortie de la notification vers des systèmes spécifiés après un événement spécifié.

Les messages de diffusion peuvent être envoyés à des systèmes Windows uniquement en spécifiant le système cible. Les messages de diffusion sont limités à 1 000 caractères ; le format court est donc conseillé.

Méthode d'envoi d'e-mail

Vous pouvez envoyer un e-mail avec la sortie d'une notification à des destinataires spécifiés. Indiquez l'adresse e-mail complète du destinataire.

> **IMPORTANT :**
> En raison des fonctions de sécurité de Microsoft Outlook, l'utilisation de la méthode d'envoi d'e-mail peut provoquer un arrêt de réponse du service CRS. Pour plus d'informations, reportez-vous au document *Annonces sur les produits, notes sur les logiciels et références HPE Data Protector*. Donc, la méthode recommandée pour l'envoi de notifications par e-mail est SMTP.

> **REMARQUE :**
> Si Microsoft Exchange Server 2007 est installé sur le Gestionnaire de cellule Data Protector, la méthode d'envoi de notifications par e-mail ne fonctionne pas. Dans ce cas, utilisez la méthode d'envoi e-mail (SMTP).

Sur les systèmes Windows

Pour envoyer une notification par e-mail à partir d'un système Windows, vous devez disposer d'un profil de messagerie. Vous pouvez utiliser un profil de messagerie existant ou en créer un nouveau, nommé `OmniBack`.

Pour utiliser un profil de messagerie existant, ajoutez la ligne suivante au fichier : Data Protector `omnirc`

`OB2_MAPIPROFILE=`*`existing_MAPI_profile_name`*

Sur les systèmes UNIX

Le sous-système d'e-mail doit être configuré et exécuté sur un système UNIX.

En raison des limites de ce système d'exploitation, les caractères internationaux présents dans les notifications électroniques localisées peuvent ne pas s'afficher correctement sur les systèmes UNIX dans le cas de transmissions entre des systèmes n'utilisant pas les mêmes paramètres régionaux.

Méthode d'envoi d'e-mail (SMTP)

Vous pouvez envoyer un e-mail avec la sortie d'une notification à des destinataires spécifiés. Indiquez l'adresse e-mail complète du destinataire.

Il s'agit de la méthode d'envoi d'e-mail recommandée.

Par défaut, l'adresse du serveur SMTP utilisé pour l'envoi des notifications correspond à l'adresse IP du Gestionnaire de cellule. Pour modifier l'adresse, éditez l'option globale `SMTPServer` . Le serveur SMTP doit être accessible à partir du système du Gestionnaire de cellule, mais peut ne pas appartenir à la cellule Data Protector.

Méthode d'envoi externe

La méthode d'envoi de script externe permet d'effectuer la sortie de la notification sur votre propre script. Le script reçoit la sortie comme entrée standard (STDIN). Le format recommandé pour le traitement du script est le format *tab*.

Le script, situé sur le système du Gestionnaire de cellule, doit résider dans le répertoire des commandes administratives Data Protector par défaut. N'indiquez que le nom du script, pas le chemin d'accès.

Notez que seules les extensions `.bat`, `.exe` et `.cmd` sont prises en charge pour les scripts externes sur les systèmes Windows. Pour exécuter un script avec une extension non prise en charge (par exemple, `.vbs`), créez un fichier de commandes qui démarre le script. Configurez ensuite Data Protector pour exécuter le fichier de commandes en tant que script externe, qui lance à son tour le script avec l'extension non prise en charge.

Vous pouvez également utiliser cette méthode d'envoi pour réaliser une éjection planifiée des supports spécifiés.

Méthode d'envoi Journaliser dans un fichier

La méthode d'envoi Journaliser dans un fichier permet d'envoyer un fichier contenant la sortie de la notification lorsqu'un événement spécifié se produit.

Le fichier est envoyé au système du Gestionnaire de cellule. Vous devez préciser le nom du fichier vers lequel vous souhaitez envoyer la notification. Le fichier sera écrasé s'il existe.

Méthode d'envoi Journal d'événements Data Protector

Par défaut, toutes les notifications sont envoyées au journal d'événements Data Protector. Le Journal Evénement Data Protector est accessible uniquement pour les utilisateurs Data Protector dans le groupe d'utilisateurs `admin` et aux utilisateursData Protector qui détiennent les droits utilisateur de Rapport et de Notification. Vous pouvez afficher ou supprimer tous les événements du journal d'événements Data Protector.

Méthode d'envoi SNMP

La méthode d'envoi SNMP vous permet d'envoyer une interruption SNMP avec la sortie de la notification lorsqu'un événement spécifié se produit. L'interruption SNMP peut être ensuite traitée par des applications utilisant les interruptions SNMP.

Sur les systèmes Windows

Sur un Gestionnaire de cellule Windows, les interruptions SNMP sont envoyées aux systèmes définis dans la configuration d'interruptions SNMP Windows. Vous devez configurer les interruptions SNMP

Windows pour pouvoir utiliser la méthode d'envoi SNMP sur les systèmes Windows.

Sur les systèmes UNIX

Sur un Gestionnaire de cellule UNIX, les interruptions SNMP sont envoyées aux systèmes configurés dans la notification.

Méthode d'envoi Utiliser groupe de rapports

La méthode d'envoi Utiliser groupe de rapports vous permet d'exécuter un groupe de rapports lorsqu'un événement spécifié se produit.

Configuration des notifications

Pour configurer une notification, vous devez lui donner un nom, spécifier son type, un niveau de message, une méthode d'envoi et un destinataire. Tous les autres paramètres d'entrée dépendent du type de la notification.

Conditions préalables

Vous devez faire partie du groupe d'utilisateurs `admin`ou disposer des droits d'utilisateur de rapports et notifications.

Procédure

1. Dans la liste de contexte, sélectionnez **Création de rapports**.
2. Cliquez avec le bouton droit sur **Notifications**, puis cliquez sur **Ajouter notification** pour lancer l'assistant.
3. Les options de l'assistant dépendent de la notification que vous avez sélectionnée. Par exemple, toutes les options disponibles pour la notification Espace IDB insuffisant ne le sont pas pour la notification Limites IDB. Cliquez sur **Suivant** autant de fois que cela est nécessaire pour atteindre la dernière page de l'assistant.
4. Cliquez sur **Terminer** pour quitter l'assistant

La notification est envoyée selon la méthode d'envoi spécifiée lorsque l'événement indiqué se produit.

> **CONSEIL :**
> Pour déclencher un groupe de rapports par une notification, configurez un groupe de rapports, puis la notification avec la méthode d'envoi Utiliser le groupe de rapports.

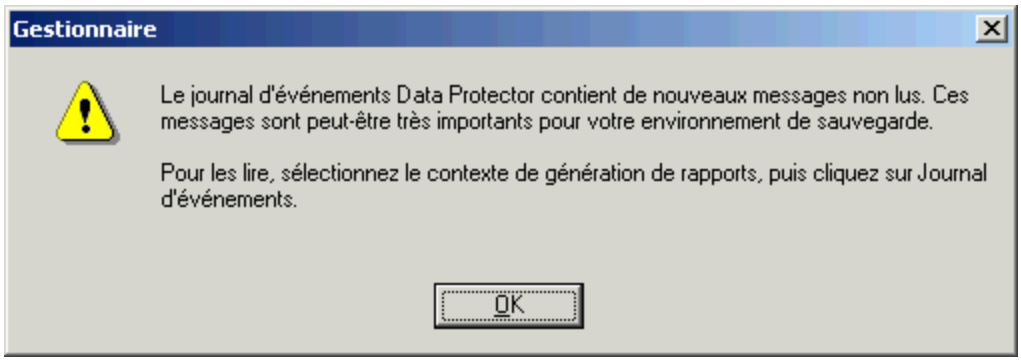
A propos du journal d'événements HPE Data Protector

Le journal d'événements Data Protector constitue un mécanisme de gestion des événements centralisé, chargé de traiter des événements spécifiques qui se sont produits lors du fonctionnement de Data Protector. Le mécanisme de consignation d'événements de Data Protector consigne deux types d'événements : ceux déclenchés par un processus et ceux déclenchés par un utilisateur. Les

événements sont consignés dans le Gestionnaire de cellule, dans le fichier `Ob2EventLog.txt`, stocké dans le répertoire par défaut Data Protector des fichiers journaux .

L'affichage du journal d'événements Data Protector avec l'observateur de journal d'événements peut vous aider à résoudre des problèmes.

Lorsque l'interface utilisateur graphique Data Protector est démarrée par un utilisateur et si celui-ci n'a pas vu que le journal d'événements Data Protector contenait de nouvelles notifications, le message suivant s'affiche :



L'interface Data Protector bascule automatiquement sur le contexte Rapports.

Les points suivants peuvent contenir des informations supplémentaires :

- Vous devez faire partie du groupe d'utilisateurs `admin` ou disposer des droits d'utilisateur de rapports et de notifications.
- Le journal d'événements de Data Protector n'est pas actualisé automatiquement. Pour afficher les nouveaux messages, actualisez-le à l'aide de la touche **F5**.

Evénements déclenchés par un processus

Un événement est consigné par la fonctionnalité de notifications.

Evénements déclenchés par un utilisateur

Un événement est consigné lorsqu'un utilisateur exécute une opération spécifique ou un ensemble d'opérations dans l'interface. Cet ensemble d'opérations inclut les modifications des spécifications de sauvegarde, de copie d'objet et de consolidation, les opérations sur les utilisateurs et les groupes d'utilisateurs, la création et la modification de la configuration liée aux périphériques et aux supports, et les opérations d'installation à distance.

Par défaut, la consignation des événements déclenchés par un utilisateur est désactivée. Pour l'activer, définissez l'option globale `EventLogAudit` sur 1.

Dans un environnement MoM, si l'option globale est définie sur 1, les événements ne sont consignés que sur le système Gestionnaire de cellule local.

Accès à l'observateur de journal d'événements

L'observateur de journal d'événements Data Protector vous permet de parcourir les événements enregistrés.

Conditions préalables

Vous devez faire partie du groupe d'utilisateurs `admin` ou disposer des droits d'utilisateur de rapports et de notifications.

Procédure

1. Dans la liste de contexte, sélectionnez **Création de rapports**.
2. Dans la fenêtre de navigation, développez **Génération de rapports**.
3. Pour l'afficher, sélectionnez **Journal d'événements**.

Suppression du contenu de l'observateur de journal d'événements

> **REMARQUE :**
> La suppression du contenu de l'observateur de journal d'événements ne supprime pas le contenu du fichier `Ob2EventLog.txt`.

Conditions préalables

Vous devez faire partie du groupe d'utilisateurs Admin ou disposer des droits d'utilisateur de rapports et notifications.

Procédure

1. Dans la liste de contexte, sélectionnez **Création de rapports**.
2. Dans la fenêtre de navigation, développez **Génération de rapports**.
3. Cliquez avec le bouton droit de la souris sur **Journal d'événements** et sélectionnez **Journal d'événements vide** pour supprimer toutes les entrées de l'observateur de journal d'événements.

A propos de l'audit

Data Protector fournit une fonction d'audit des sessions de sauvegarde qui permet de stocker des informations infalsifiables et non modifiables sur toutes les tâches de sauvegarde exécutées sur des périodes définies par l'utilisateur pour l'ensemble de la cellule Data Protector. Ces informations peuvent être récupérées sur demande, sous une forme intégrale et imprimable, à des fins d'audit ou d'administration.

Vous pouvez activer les informations d'audit et définir la période de conservation des fichiers journaux d'audit en modifiant les options globales `AuditLogEnable` et `AuditLogRetention`.

Génération d'un rapport d'audit

Pour créer un rapport d'audit, exécutez la procédure ci-dessous.

> **REMARQUE :**
> Dans un environnement MoM, vous devez générer des rapports d'audit pour chaque Gestionnaire de cellule séparément.

Procédure

1. Dans la liste de contexte, cliquez sur **Base de données interne**.
2. Dans la fenêtre de navigation, cliquez sur l'élément **Audit** pour ouvrir la page correspondante.
3. Dans la liste déroulante Intervalle de recherche, sélectionnez l'une des valeurs (par exemple `Last week`).
4. Cliquez sur le bouton de **Mise à jour** pour afficher la liste de toutes les sessions de sauvegarde effectuées au cours de la période sélectionnée.
5. Sélectionnez une session spécifique dans la liste pour afficher des informations détaillées sur les objets et les supports utilisés dans les parties centrale et inférieure de la page de propriétés Audit.

Vérification du fonctionnement normal de Data Protector

Vérifications effectuées par Data Protector

Data Protector propose son propre mécanisme de vérification et de maintenance, qui effectue des tâches de maintenance et des vérifications quotidiennement. La maintenance quotidienne exécute une série de commandes qui purgent les données obsolètes de nombreuses sections de la base de données interne de Data Protector.

Par défaut, la maintenance quotidienne est effectuée à midi chaque jour. Elle ne purge pas toutes les parties de l'IDB, seulement celles pouvant l'être sans accès exclusif à l'IDB.

Tâches de maintenance

Tous les jours à midi par défaut, Data Protector :

- Supprime les fichiers binaires DC, les sessions et messages liés obsolètes en exécutant les commandes `omnidbutil -purge` suivantes :
  - `-dcbf`
  - `-sessions`

  - `-messages`

  L'option `-sessions` de maintenance quotidienne dépend de la configuration de l'option globale `KeepObsoleteSessions` et de l'option `messages` sur l'option globale `KeepMessages` .

- Trouve les supports libres (non protégés) dans les pools de supports dans lesquels les options **Utiliser pool libre** et **Déplacer support libre vers pool libre** sont définies, et désaffecte le support libre d'un pool libre en exécutant la commande `omnidbutil -free_pool_update`.
- Vérifie la protection pour le support et supprime le support et les emplacements de support correspondants. Si le support est exporté depuis l'IDB, l'emplacement n'est plus connu pour l'IDB, et Data Protector ne peut donc pas libérer le stockage pour un tel support. Le support doit être supprimé manuellement du stockage et les emplacements de support devraient également être supprimés manuellement depuis le contexte du périphérique.

Pour plus d'informations, reportez-vous à la page de manuel `omnidbutil` ou à la *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Vérifications

Tous les jours à 12h30 par défaut, Data Protector démarre les vérifications pour les notifications suivantes :

- Peu d'espace dans la base de données interne
- Limites IDB
- Sauvegarde IDB requise
- Supports libres insuffisants
- Échec de l'auto-test
- Échec de la vérification de l'utilisateur (si configurée)
- Événements inattendus
- Avertissement concernant la licence
- La licence arrive à expiration

Tous les lundis à 12h30 par défaut, Data Protector démarre la vérification pour la notification suivante :

- Réorganisation de l'IDB requise

Par défaut, toutes les notifications déclenchées sont envoyées au journal d'événements de Data Protector.

> **CONSEIL :**
> Vous pouvez modifier les valeurs de planification par défaut pour les tâches et vérifications de maintenance. Utilisez les options globales `DailyMaintenanceTime` et `DailyCheckTime` respectivement avec la notation d'horloge à vingt-quatre heures.

Quelles vérifications dois-je effectuer ?

En plus des vérifications que Data Protector effectue par défaut, il est conseillé d'effectuer des vérifications régulières. De cette façon, vous vous assurez que Data Protector fonctionne correctement et que vous identifiez les problèmes potentiels avant qu'ils ne surviennent.

CONSEIL :
Vous pouvez automatiser ces vérifications en développant des scripts et en utilisant la notification Échec de la vérification de l'utilisateur.

Certaines des vérifications (par exemple, les commandes `omnihealthcheck` et `omnitrig -run_checks`) sont déjà réalisées en tant qu'éléments du mécanisme de contrôle et de maintenance Data Protector.

Pour plus d'informations sur les commandes utilisées, reportez-vous aux pages de manuel appropriées ou au document *Guide de référence de l'interface de ligne de commande HPE Data Protector*.

Quelles vérifications effectuer ?	**Qu'est-ce qui est vérifié et comment ?**
Vérifier le Gestionnaire de cellule de Data Protector	Les vérifications suivantes sont réalisées avec succès si le code de sortie de la commande est `0` (OK). Les valeurs de sortie autres que 0 indiquent que la vérification a échoué. 1. Exécutez la commande `omnihealthcheck` pour vérifier si : • les services Data Protector (CRS, MMD, hpdb-idb, hpdp-idb-cp, hpdp-as, omnitrig, KMS et Inet) sont actifs • la base de données de gestion des supports Data Protector est cohérente • au moins une image de sauvegarde de l'IDB existe Le code de sortie de la commande est `0` (OK) uniquement si les trois vérifications sont réalisées avec succès (le code de sortie pour chaque vérification était `0`). 2. Exécutez la commande `omnidbcheck -quick` pour vérifier l'IDB.
Vérifier si les sauvegardes ont bien été effectuées	1. Exécutez le test de sauvegarde pour les spécifications de sauvegarde cruciales. Les tests réussis montrent que : • Tous les clients de la spécification de sauvegarde sont accessibles à partir du Gestionnaire de cellule. • Tous les fichiers sont accessibles. • La quantité de données à sauvegarder est déterminée. • Tous les périphériques de sauvegarde sont correctement configurés. Notez que le test n'est pas pris en charge pour certaines intégrations ni pour ZDB. 2. Exécutez la commande `omnirpt -report dl_sched` pour vérifier si les spécifications de sauvegarde sont programmées conformément à votre politique de sauvegarde. La commande répertorie toutes les spécifications de sauvegarde et leurs planifications.

Vérifier l'installation Data Protector	Vérifiez l'installation en utilisant l'interface graphique Data Protector, contexte Clients, pour vérifier si les composants logiciels de Data Protector sont opérationnels sur le Gestionnaire de cellule ou les systèmes clients.
Vérifier les fichiers journaux de Data Protector	Inspectez les fichiers journaux Data Protector suivants et identifier les problèmes possibles : • `event.log` • `debug.log` • `purge.log`
Exécuter la vérification des notifications	Par défaut, Data Protector démarre la vérification pour la notification suivante une fois par jour. Toutes les notifications déclenchées sont envoyées au journal d'événements de Data Protector. Vous pouvez également exécuter la commande `omnitrig -run_checks` pour démarrer les vérifications pour les notifications: • Peu d'espace dans la base de données interne • Supports libres insuffisants • Événements inattendus • Échec de l'auto-test • Limites IDB • Sauvegarde IDB requise • Réorganisation de l'IDB requise • La licence arrive à expiration • Avertissement concernant la licence • Échec de la vérification de l'utilisateur (si configurée)
Vérifier les autres ressources système	Inspectez les fichiers journaux du système d'exploitation suivants et identifiez les problèmes possibles : **Systèmes Windows :** la visionneuse d'événements Windows et ses journaux de sécurité, système et d'applications **Systèmes UNIX :** `/var/adm/syslog/syslog.log`
Vérifier le fichier de récupération de l'IDB	Vérifiez le fichier de récupération de l'IDB, `obrindex.dat`, afin de vous assurer que l'IDB et les fichiers de configuration nécessaires pour la récupération réussie d'un Responsable de Cellule sont créés régulièrement.

Comment automatiser les vérifications

Vous pouvez automatiser les vérifications en utilisant un script et en configurant la notification Echec de la vérification de l'utilisateur.

La notification Echec de la vérification de l'utilisateur exécute la commande ou le script spécifié en tant que paramètre d'entrée dans cette notification, et déclenche la notification si la valeur de retour de certaines commandes exécutées dans le script est différente de `0`. Vous recevez la notification via la méthode d'envoi sélectionnée.

La commande ou le script doit se trouver sur le système d'application dans le répertoire de commandes d'administration par défaut de Data Protector.

La notification Echec de la vérification de l'utilisateur configurée est démarrée chaque jour dans le cadre des vérifications quotidiennes de Data Protector et, si déclenchée, est envoyée au journal des événements de Data Protector.

Documentation HPE Data Protector

> **REMARQUE :**
> La documentation disponible sur le site Web du support HPE à l'adresse https://softwaresupport.hpe.com/ contient les dernières mises à jour et corrections.

Vous pouvez accéder au kit de documentation HPE Data Protector à partir des emplacements suivants :

- Répertoire d'installation de HPE Data Protector.

  Systèmes Windows : *répertoire_Data_Protector*\docs

  Systèmes UNIX :/opt/omni/doc/C
- Menu **Aide** du GUI HPE Data Protector .
- Site Web d'assistance HPE à l'adresse https://softwaresupport.hpe.com/

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										
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 "HPE 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

Abréviation	Elément de documentation	
		logiciel Data Protector, en prenant en 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, MySQL, SAP R3, SAP MaxDB, and 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.

Abréviation	Elément de documentation	
ZDB Admin	Guide de l'administrateur ZDB	Ce guide décrit comment configurer et utiliser l'intégration de Data Protector avec les baies de disque. 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
Microsoft Volume Shadow Copy Service (VSS)	Intégration VSS

Application logicielle	Guides
Serveur NDMP (Network Data Management Protocol)	Guide d'intégration
Serveur Oracle	Guide d'intégration, ZDB IG
Serveur MySQL	Guide d'intégration
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 HPE P4000 SAN	Concepts, ZDB admin, Guide d'intégration
Famille de baies de disques HPE P6000 EVA	Tous ZDB, Guide d'intégration
Famille de baies de disque HPE P9000 XP	Tous ZDB, Guide d'intégration
3PAR StoreServ Storage HPE	Concepts, ZDB admin, Guide d'intégration
Stockage NetApp	Concepts, ZDB Admin, ZDB IG
EMC VNX	Concepts, ZDB Admin, ZDB IG

Famille de baies de disque	Guides
EMC VMAX	Concepts, ZDB Admin, ZDB IG

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 de l'administrateur (HPE 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 AutonomyTPFeedback@hpe.com.

Nous sommes heureux de recevoir vos commentaires !