Guide des concepts
HP OpenView Storage Data Protector

Date de publication : octobre 2004

Référence constructeur : B6960-92105

Version A.05.50

Informations légales

Sommaire

Sommaire

Sommaire

Sommaire

7. Fonctionnement de Data Protector

8. Intégration avec les applications de base de données

9. Sauvegarde directe

Sommaire

Informations sur cette documentation

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

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

Tableau 1 Informations sur cette édition

Référence	Date de publication	Produit
B6960-92080	Mai 2003	Data Protector version A.05.10
B6960-92105	Octobre 2004	Data Protector version A.05.50

Conventions typographiques

Dans ce manuel, les conventions typographiques suivantes seront utilisées :

Tableau 2

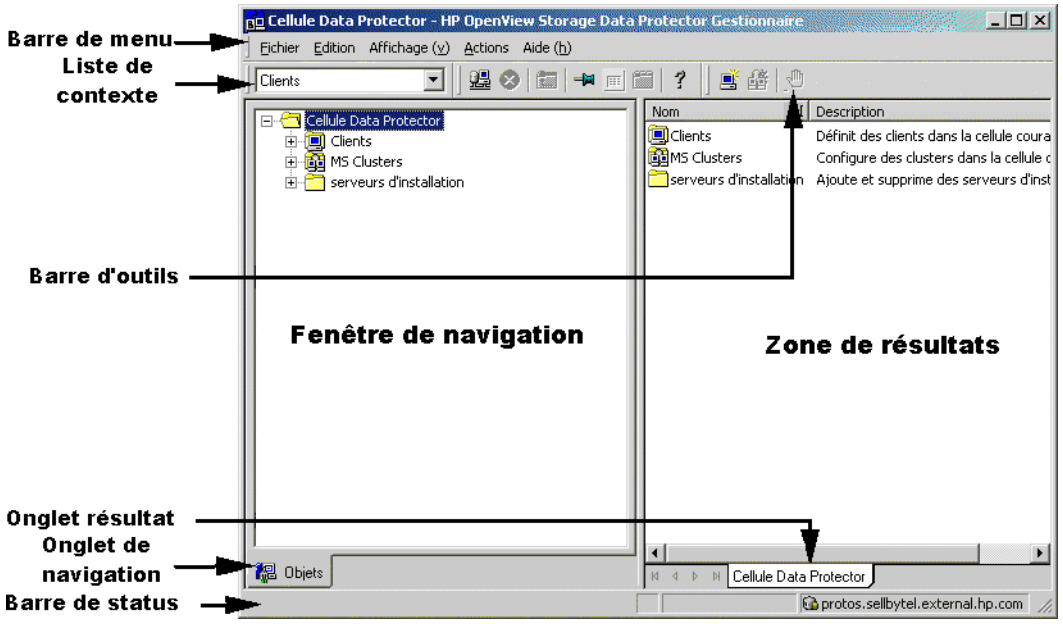
Convention	Signification	Exemple
Italiques	Titres de manuels ou d'autres documents, titres sur les différentes pages des manuels.	Pour plus d'informations, reportez-vous au *Guide d'intégration de HP OpenView Storage Data Protector*.
	Fait ressortir le texte.	Vous *devez* suivre la procédure décrite.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

Tableau 2

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

L'interface graphique utilisateur de Data Protector se présente de la même façon sous Windows et UNIX. Pour en savoir plus sur l'interface graphique utilisateur de Data Protector, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Figure 1 Interface graphique utilisateur de Data Protector



Contacts

Informations générales

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

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

Support technique

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

http://support.openview.hp.com/support.jsp

http://www.hp.com/support

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

http://support.openview.hp.com/patches/patch_index.jsp

Pour plus d'informations sur les correctifs Data Protector requis, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

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

Vos commentaires sur la documentation

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

http://ovweb.external.hp.com/lpe/doc_serv/

Formation

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

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

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

Documentation Data Protector

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

Manuels

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

Guide des concepts HP OpenView Storage Data Protector

Ce manuel décrit les concepts Data Protector et fournit des informations de fond sur le fonctionnement du logiciel. Il est destiné à être utilisé avec le *Guide de l'administrateur de HP OpenView Storage Data Protector*, lequel met l'accent sur les tâches du logiciel.

Guide de l'administrateur de HP OpenView Storage Data Protector

Ce manuel décrit les tâches de configuration et de gestion de l'administrateur chargé de la sauvegarde de systèmes ; ces tâches comprennent notamment la configuration de périphériques de sauvegarde, la gestion de support, la configuration des sauvegardes et la restauration des données.

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

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

Guide d'intégration de HP OpenView Storage Data Protector

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

- *Guide d'intégration de HP OpenView Storage Data Protector pour les applications Microsoft : SQL Server 7/2000, Exchange Server 5.x, Exchange Server 2000/2003 et Volume Shadow Copy Service*

  Ce manuel décrit les intégrations de Data Protector avec les applications Microsoft suivantes : Microsoft Exchange Server 2000/2003, Microsoft Exchange Server 5.x, Microsoft SQL Server 7/2000 et Volume Shadow Copy Service.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ce manuel décrit la configuration et l'utilisation de l'intégration de Data Protector à HP StorageWorks Virtual Array, HP StorageWorks Enterprise Virtual Array, EMC Symmetrix Remote Data Facility et TimeFinder, ainsi qu'à HP StorageWorks Disk Array XP. Il s'adresse aux opérateurs ou aux administrateurs de sauvegarde. Il décrit la sauvegarde avec temps d'indisponibilité nul, la restauration instantanée, ainsi que la restauration de systèmes de fichiers et d'images disque.

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

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

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

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

HP OpenView Storage Data Protector Media Operations User's Guide

Ce manuel vous indique comment procéder au suivi et à la gestion des supports de stockage hors ligne. Il s'adresse aux administrateurs réseau responsables de la maintenance et de la sauvegarde de systèmes. Il décrit l'installation et la configuration de l'application, la réalisation des opérations quotidiennes relatives aux supports et la production de rapports.

Notes de publication du logiciel HP OpenView Storage Data Protector

Ce manuel fournit une description des nouveautés de HP OpenView Storage Data Protector A.05.50. Il comporte également des informations sur les configurations prises en charges (périphériques, plates-formes et intégrations de bases de données en ligne, SAN et ZDB), des correctifs requis et des limitations, ainsi que des problèmes connus et de leurs solutions. Une version mise à jour des configurations prises en charge est disponible à l'adresse http://www.openview.hp.com/products/datapro/spec_0001.html.

Aide en ligne

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

Contenu des manuels

Le *Guide des concepts HP OpenView Storage Data Protector* décrit les concepts de Data Protector. La lecture de ce manuel donne une bonne compréhension des concepts fondamentaux et du modèle sur lequel est construit Data Protector.

Public

Ce manuel s'adresse aux utilisateurs qui s'intéressent aux concepts de fonctionnement de Data Protector et aux personnes responsables de la planification de stratégies de sauvegarde pour leur entreprise. Selon le niveau de détail requis, vous pouvez également utiliser ce manuel conjointement au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Organisation

Le manuel est organisé de la façon suivante :

Chapitre 1 “A propos de la sauvegarde et de Data Protector” à la page 1.

Chapitre 2 “Planification de la stratégie de sauvegarde” à la page 27.

Chapitre 3 “Gestion des supports et périphériques” à la page 133.

Chapitre 4 “Utilisateurs et groupes d’utilisateurs” à la page 195.

Chapitre 5 “La base de données interne de Data Protector” à la page 201.

Chapitre 6 “Gestion des services” à la page 231.

Chapitre 7 “Fonctionnement de Data Protector” à la page 253.

Chapitre 8 “Intégration avec les applications de base de données” à la page 271.

Chapitre 9 “Sauvegarde directe” à la page 281.

Chapitre 10 “Sauvegarde sur disques” à la page 295.

Chapitre 11 “Concepts Split Mirror” à la page 303.

Chapitre 12 “Concepts de snapshot” à la page 315.

Chapitre 13 “Microsoft Volume Shadow Copy Service” à la page 331.

Annexe A “Scénarios de sauvegarde” à la page A-1.

Annexe B “Informations supplémentaires” à la page B-1.

Glossaire Définition des termes utilisés dans ce manuel

1 A propos de la sauvegarde et de Data Protector

Description du chapitre

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

Il s'organise comme suit :

A propos de Data Protector

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

- **Une architecture évolutive et d'une grande flexibilité**

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

- **Une administration facile et centralisée**

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

- **Une fonction de sauvegarde haute performance**

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

- **La prise en charge des environnements mixtes**

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

- **Une installation facile pour les environnements mixtes**

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

- **La grande disponibilité des données**

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

  — Intégration avec les clusters pour garantir un fonctionnement sécurisé et la possibilité de sauvegarder des nœuds virtuels. Pour obtenir une liste des clusters pris en charge, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

  — Activation du Gestionnaire de cellule Data Protector lui-même pour une exécution sur un cluster.

  — Prise en charge des API (interfaces de programmation d'application) de base de données en ligne les plus courantes.

  - — Intégration à des solutions évoluées haute disponibilité, telles que EMC Symmetrix, HP StorageWorks Disk Array XP, HP StorageWorks Virtual Array ou HP StorageWorks Enterprise Virtual Array.
  - — Mise à disposition de diverses méthodes de récupération après sinistre pour les plates-formes Windows et UNIX.
  - — Communication de méthodes de duplication des données sauvegardées pendant et après la sauvegarde en vue d'améliorer la tolérance aux pannes ou à des fins de redondance.

- **Une procédure de restauration facile**

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

- **Des opérations automatisées ou sans surveillance**

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

  Cette fonctionnalité est complétée par la prise en charge de très grandes bibliothèques, ce qui permet un fonctionnement sans surveillance sur plusieurs jours ou semaines (rotation automatique des supports).

  De plus, lorsque vous connectez de nouveaux disques aux systèmes, Data Protector est en mesure de les détecter automatiquement (ou de les reconnaître) et de les sauvegarder. Il est donc inutile d'adapter les configurations de sauvegarde manuellement.

- **Gestion des services**

  Data Protector est la première solution de gestion de sauvegarde et de restauration à prendre en charge la gestion des services. L'intégration aux solutions de gestion du temps de réponse des applications (ARM) et d'intégration des sources de données (DSI) contribue efficacement à

la gestion du niveau de service (SLM) et au respect des contrats de niveau de service (SLA) en fournissant des données pertinentes aux systèmes de gestion et de planification.

L'intégration DSI fournit une série de fichiers scripts et de configuration à partir desquels les utilisateurs peuvent voir comment ajouter leurs propres requêtes à l'aide des fonctions de génération de rapports de Data Protector.

- **Les fonctions de surveillance, de génération de rapports et de notification**

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

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

- **L'intégration aux applications de base de données en ligne**

  Data Protector fournit la sauvegarde en ligne des objets des bases de données Microsoft Exchange Server, Microsoft SQL Server, Oracle, Informix, SAP R/3, Lotus Notes/Domino Server, IBM DB2 UDB et Sybase. Pour obtenir la liste des versions prises en charge pour un système d'exploitation particulier, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

- **L'intégration avec d'autres produits**

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

Pour obtenir une documentation détaillée décrivant les fonctions de Data Protector, y compris les intégrations, ainsi que les informations les plus récentes en termes de prise en charge des intégrations et des plates-formes, reportez-vous à la page d'accueil de HP OpenView Storage Data Protector à l'adresse http://www.openview.hp.com/products/datapro/spec_0001.html.

Présentation des sauvegardes et des restaurations

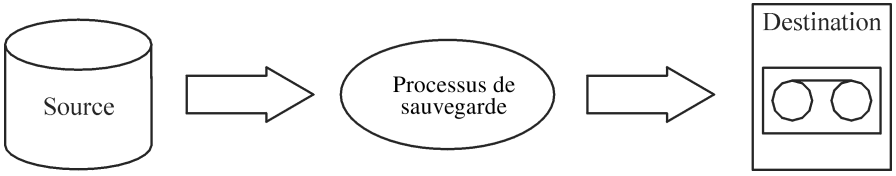
Vous trouverez dans cette section les principes de base relatifs aux concepts de sauvegarde et de restauration.

Qu'est-ce qu'une sauvegarde ?

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

Pour obtenir une présentation globale d'une sauvegarde, reportez-vous à la figure 1-1 ci-dessous.

Figure 1-1 **Processus de sauvegarde**



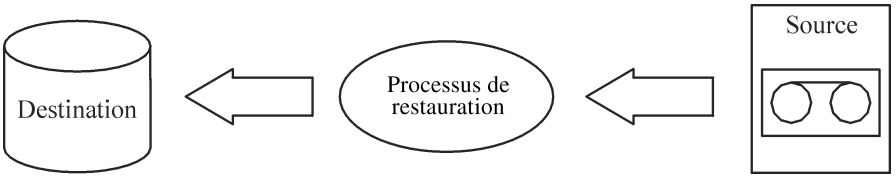
Dans la plupart des cas, la **source** correspond à des données enregistrées sur un disque, par exemple des fichiers, des répertoires, des bases de données et des applications. Si la sauvegarde est réalisée dans l'optique d'une récupération après sinistre, il faut qu'elle soit cohérente.

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

Qu’est-ce qu’une restauration ?

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

Figure 1-2 Processus de restauration

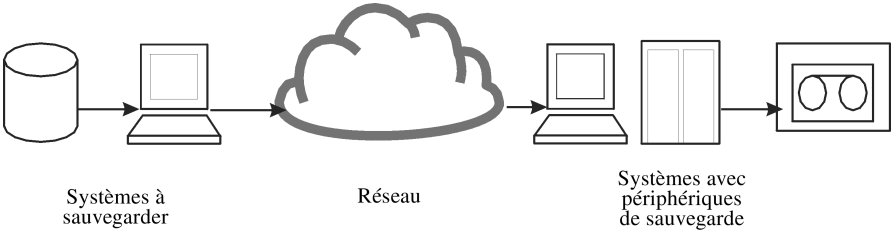


La **source** est une copie de sauvegarde. Une application de restauration est un logiciel qui inscrit les données sur un point de destination. La **destination** est généralement un disque sur lequel les données d’origine sont écrites.

Sauvegarde d’un environnement réseau

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

Figure 1-3 Sauvegarde réseau



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

- Raccorder des périphériques de sauvegarde à n'importe quel système du réseau.

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

Sauvegarde directe

Une sauvegarde **directe** est une sauvegarde par laquelle vous envoyez les données directement à partir du disque vers la bande dans le réseau SAN, sans impliquer de serveur de sauvegarde dédié pour le mouvement des données. La sauvegarde directe Data Protector minimise l'impact de la sauvegarde sur les serveurs de production par l'utilisation de technologies de miroirs basées sur le matériel et ne provoquant pas d'ingérence.

En outre, cette solution fait appel à des capacités indépendantes du système de fichiers pour traiter les données. Cette fonction est totalement intégrée à la fonctionnalité XCOPY standard que l'on trouve dans les baies de disques et passerelles prises en charge, ce qui élimine le recours à un équipement Data mover séparé.

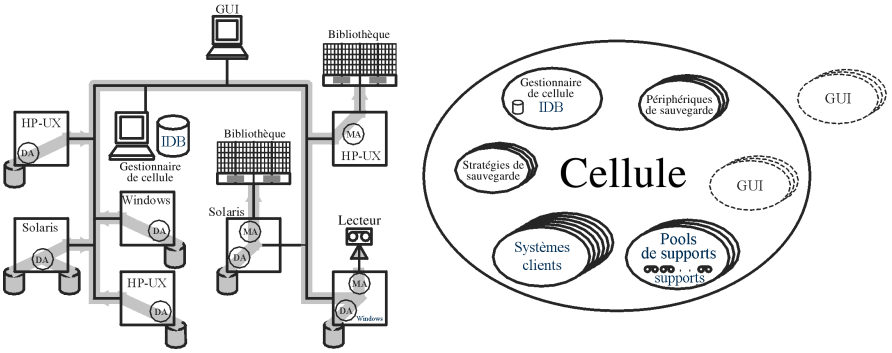
Architecture de Data Protector

La **cellule** Data Protector, représentée à la figure 1-4, est un environnement réseau doté d'un **Gestionnaire de cellule**, de **systèmes client** et de **périphériques**. Le Gestionnaire de cellule constitue le point de contrôle central sur lequel le logiciel Data Protector est installé. Après avoir installé le logiciel Data Protector, vous pouvez ajouter des systèmes à sauvegarder. Ces derniers deviennent des systèmes client de Data Protector, qui font partie de la cellule. Lorsque Data Protector sauvegarde des fichiers, il les enregistre sur des supports situés dans les périphériques de sauvegarde.

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

Data Protector simplifie les tâches de sauvegarde et de restauration. Vous pouvez effectuer une sauvegarde instantanée (ou interactive) au moyen de l'interface utilisateur de Data Protector. Vous pouvez également programmer vos sauvegardes pour qu'elles s'exécutent sans surveillance.

Figure 1-4 **Cellule Data Protector (description physique et logique)**



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

Gestionnaire de cellule

Le Gestionnaire de cellule est le système le plus important de la cellule et il :

- Gère la cellule à partir d'un point central.
- Contient la base de données IDB.

  La base de données IDB contient des informations relatives aux sauvegardes, telles que les durées des sauvegardes et les ID des supports et des sessions.
- Exécute le logiciel Data Protector brut.
- Exécute les Gestionnaires de session qui démarrent et arrêtent les sessions de sauvegarde et de restauration, et inscrivent des informations relatives aux sessions dans la base de données IDB.

Systèmes à sauvegarder

L'Agent de disque Data Protector (DA), également appelé **Agent de sauvegarde**, doit être installé sur les systèmes client que vous souhaitez sauvegarder. Pour pouvoir sauvegarder les intégrations de bases de données en ligne, vous devez installer l'**Agent d'application**. Dans le reste du manuel, le terme "Agent de disque" est utilisé pour désigner les deux agents. 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 de Data Protector et la base de données IDB.

Systèmes dotés de périphériques de sauvegarde

Un **Agent de support** Data Protector doit être installé sur les systèmes client auxquels sont connectés les périphériques de sauvegarde. Ces systèmes client sont également appelés **serveurs de lecteurs**. Un périphérique de sauvegarde peut être connecté à n'importe quel système et pas uniquement au Gestionnaire de cellule. Un Agent de support lit ou écrit des données depuis ou vers un support du périphérique et envoie ou reçoit des données de l'Agent de disque.

Systèmes dotés d'une interface utilisateur

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

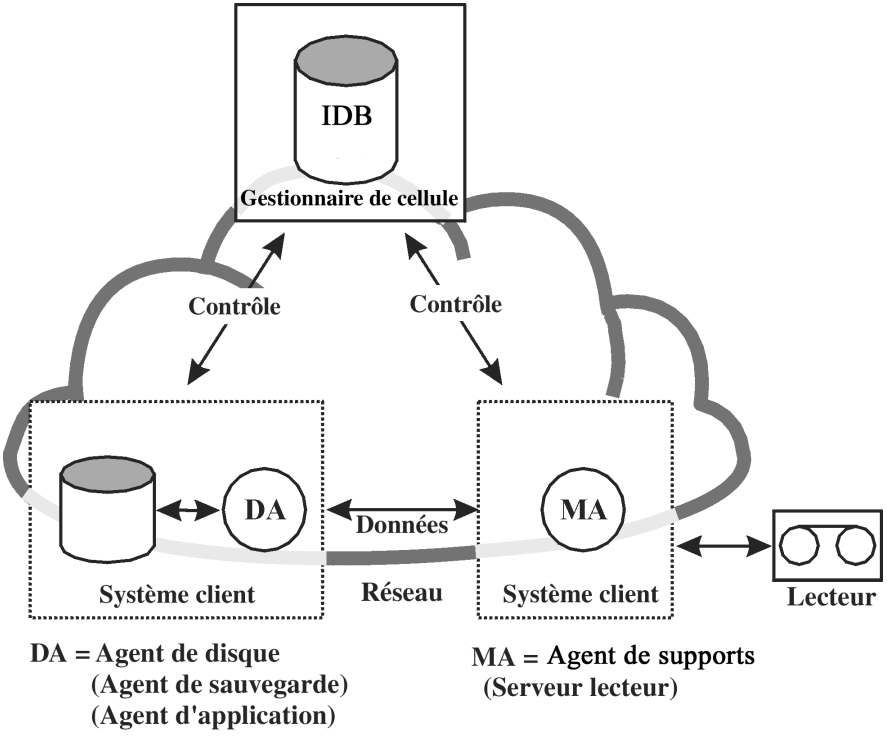
Serveur d'installation

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

Opérations effectuées dans la cellule

Le Gestionnaire de cellule Data Protector contrôle les sessions de sauvegarde et de restauration, qui effectuent respectivement toutes les actions requises pour une sauvegarde ou une restauration (voir figure 1-5).

Figure 1-5 Opération de sauvegarde ou de restauration



Sessions de sauvegarde

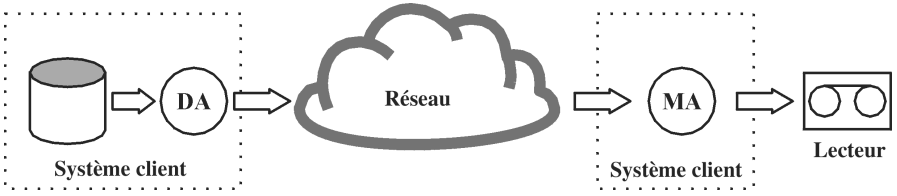
Qu'est-ce qu'une session de sauvegarde ?

Une session de sauvegarde (voir figure 1-6) est une procédure consistant à créer une copie de données sur un support de stockage. Son démarrage peut se faire de deux manières différentes : interactivement par un opérateur ou sans surveillance à l'aide du Planificateur de Data Protector.

Fonctionnement

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

Figure 1-6 Session de sauvegarde



Les sessions de sauvegarde sont généralement plus complexes que celle montrée à la figure 1-6. Plusieurs Agents de disque lisent les données de plusieurs disques en parallèle et les envoient à un ou plusieurs Agents de support. Pour obtenir des informations complémentaires sur les sessions de sauvegarde complexes, reportez-vous au Chapitre 7, "Fonctionnement de Data Protector" à la page 253.

Sessions de restauration

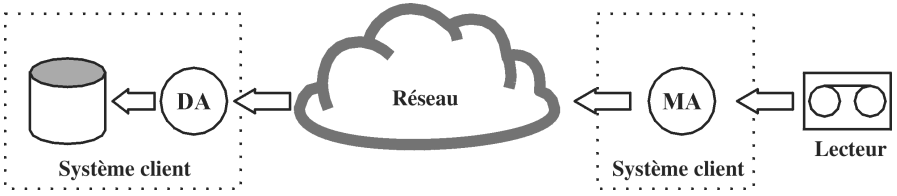
Qu'est-ce qu'une session de restauration ?

Une session de restauration (voir figure 1-7) est une procédure consistant à restaurer vers un disque des données préalablement sauvegardées. La session de restauration peut être lancée interactivement par un opérateur via l'interface utilisateur Data Protector.

Fonctionnement

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

Figure 1-7 Session de restauration



Les sessions de restauration peuvent être plus complexes que celle montrée à la figure 1-7. Pour plus d'informations sur les sessions de restauration, reportez-vous au Chapitre 7, "Fonctionnement de Data Protector" à la page 253.

Environnements d'entreprise

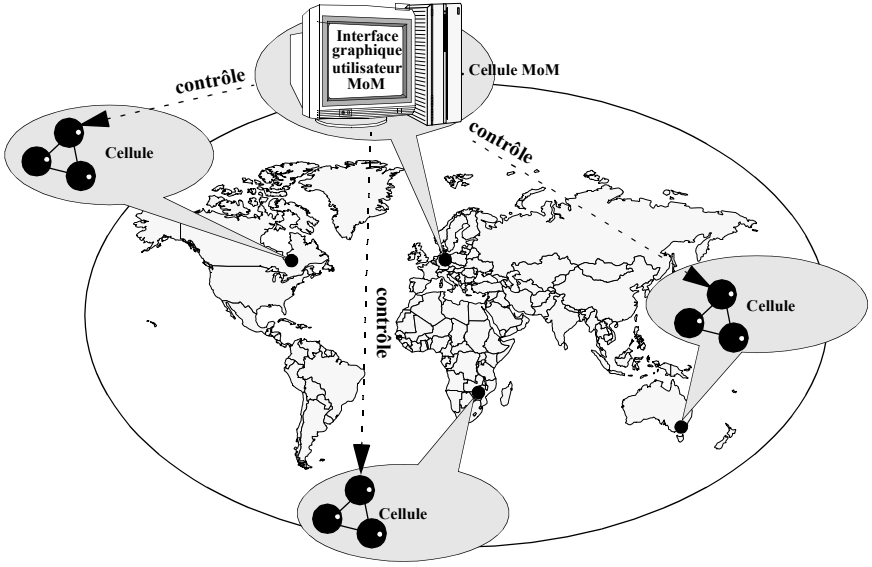
Qu'est-ce qu'un environnement d'entreprise ?

Un environnement réseau d'entreprise (voir figure 1-8) est généralement composé d'un certain nombre de systèmes provenant de différents fournisseurs et dotés de différents systèmes d'exploitation. Les systèmes peuvent être installés dans des zones géographiques et des fuseaux horaires différents. Tous les systèmes sont connectés par des réseaux (LAN ou WAN) fonctionnant à divers débits.

Quand utiliser un environnement d'entreprise ?

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

Figure 1-8 Environnement d'entreprise Data Protector étendu



La configuration et la gestion des sauvegardes dans un environnement aussi hétérogène constituent des tâches complexes. Les fonctionnalités de Data Protector ont été conçues pour les simplifier au maximum. Pour obtenir des informations complémentaires sur le Manager-of-Managers (MoM), reportez-vous à la section "MoM" à la page 17.

Séparation d'un environnement en plusieurs cellules

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

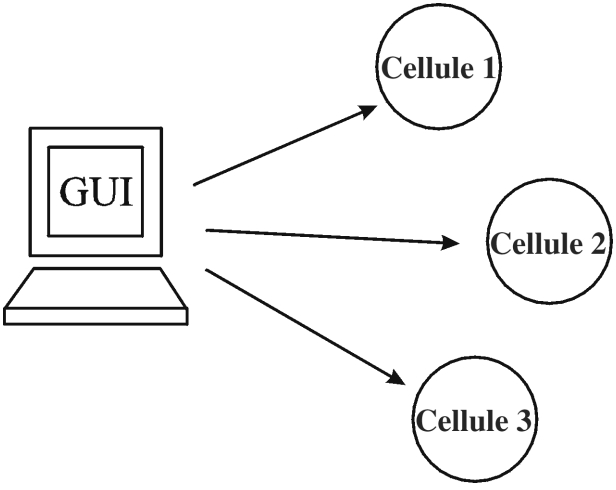
Pourquoi séparer les grands environnements en plusieurs cellules ?

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

Reportez-vous au Chapitre 2, "Planification de la stratégie de sauvegarde" à la page 27, où vous trouverez une liste de points à prendre en considération au moment de la planification de votre environnement.

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

Figure 1-9 Gestion centralisée de plusieurs cellules

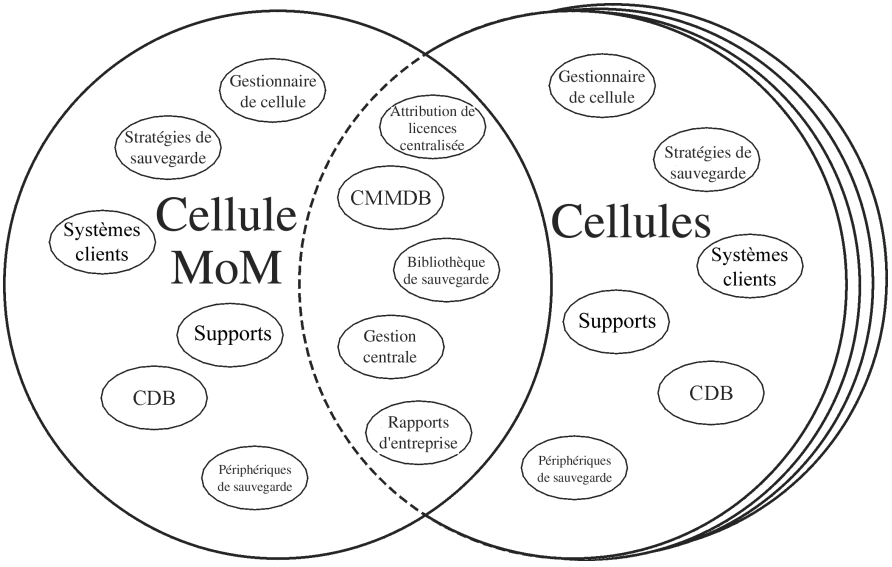


MoM

Le Manager-of-Managers de Data Protector permet de gérer les grands environnements avec plusieurs cellules. Vous pouvez ainsi regrouper plusieurs cellules au sein d'une unité plus grande appelée "environnement MoM", qui peut être gérée à partir d'un point central (voir figure 1-9). En outre, grâce au MoM, votre environnement de sauvegarde peut s'étendre de façon quasi illimitée. Vous pouvez ajouter de nouvelles cellules ou diviser des cellules existantes.

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

Figure 1-10 **Environnement Manager-of-Managers**



Le Manager-of-Managers présente les caractéristiques suivantes :

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

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

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

  La CMMDB permet à l'utilisateur de partager des supports et périphériques avec 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. Pour pouvoir être utilisée, la CMMDB doit résider dans la cellule MoM. Dans ce cas, il doit exister une connexion réseau fiable entre la cellule MoM et les autres cellules Data Protector. Notez que la centralisation de la base de données de gestion des supports n'est pas obligatoire.

- **Partage des bibliothèques**

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

- **Rapports d'entreprise**

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

Gestion des supports

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

Fonctions de gestion des supports

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

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

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

les données figurant sur le support. C'est vous qui décidez, en fonction de vos besoins, quelle doit être la structure des pools, leur nombre, et, pour chacun des pools, le type de données figurant sur les supports qui en font partie.

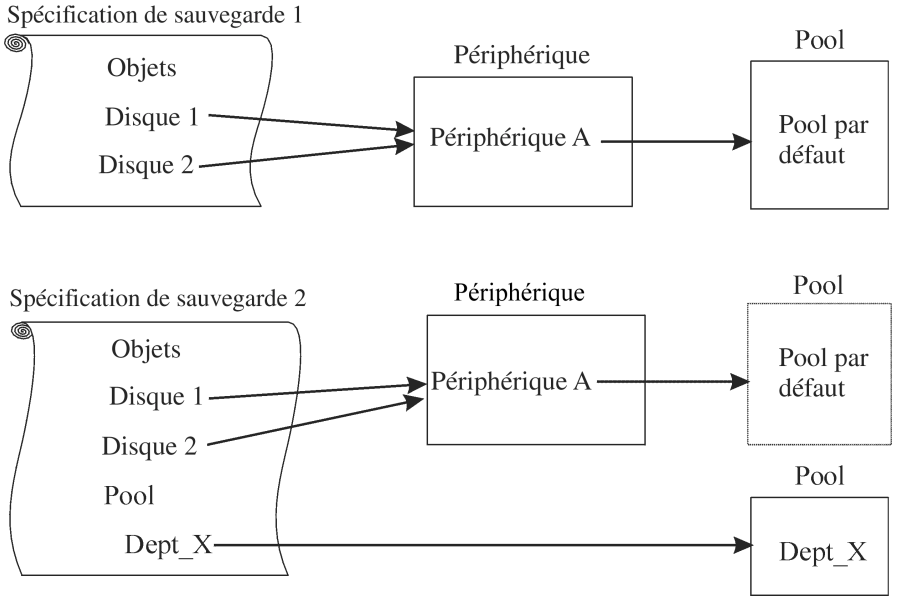
Lorsque vous configurez un périphérique, un pool de supports par défaut est spécifié. Ce pool de supports est utilisé si aucun autre pool de supports n'est défini dans la spécification de sauvegarde.

Périphériques de sauvegarde

Data Protector définit et modélise chaque périphérique comme un périphérique physique ayant des propriétés d'utilisation particulières (par exemple le pool par défaut).

Ce concept de périphérique permet de configurer facilement et en souplesse les périphériques, et de les utiliser en accord avec les spécifications de sauvegarde. La définition des périphériques est stockée dans la base de données de gestion des supports Data Protector.

Figure 1-11 **Liens entre les spécifications de sauvegarde, les périphériques et les pools de supports**



La figure 1-11 présente un schéma des relations entre les spécifications de sauvegarde, les périphériques et les pools de supports. Les périphériques sont référencés dans les spécifications de sauvegarde. Chaque périphérique est relié à un pool de supports et celui-ci peut être modifié dans la spécification de sauvegarde. Par exemple, la spécification de sauvegarde 2 fait appel au pool `Dept_X` au lieu du pool par défaut.

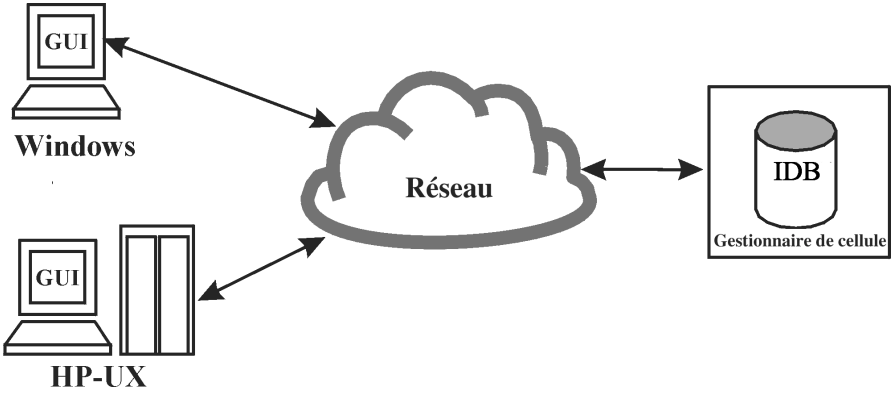
Data Protector prend en charge différents périphériques. Pour plus d'informations, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

Interfaces utilisateur

Data Protector offre un accès facile à toutes les tâches de configuration et d'administration au moyen de l'interface utilisateur Data Protector fournie pour s'exécuter sous X11/Motif sur les plates-formes UNIX et Windows. De plus, une interface de ligne de commande est également disponible sur les plates-formes UNIX et Windows.

L'architecture de Data Protector vous offre la souplesse d'installation et d'utilisation de l'interface utilisateur de Data Protector. Vous n'êtes pas tenu d'utiliser l'interface à partir du système du Gestionnaire de cellule : vous pouvez l'installer sur votre ordinateur personnel. Comme le décrit la figure 1-12, l'interface utilisateur (GUI) vous permet également de gérer les cellules Data Protector en toute transparence avec le Gestionnaire de cellule HP-UX, Solaris or Windows.

Figure 1-12 Utilisation de l'interface utilisateur de Data Protector



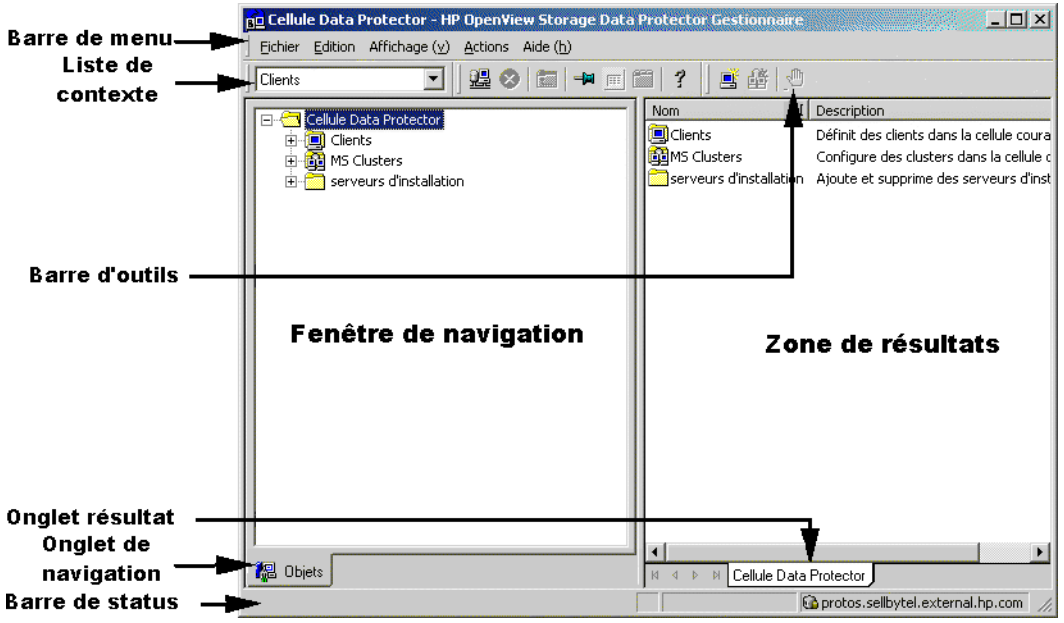
CONSEIL Dans un environnement mixte classique, installez l'interface utilisateur Data Protector sur plusieurs systèmes de l'environnement afin d'avoir accès à Data Protector à partir de plusieurs machines.

Interface graphique utilisateur de Data Protector

L'interface de Data Protector, décrite à la figure 1-13, est un outil puissant et facile à utiliser, qui présente les caractéristiques suivantes :

- Un onglet Résultats dans lequel figurent les propriétés, les listes et les assistants de configuration.
- La configuration et la gestion simples des sauvegardes d'applications de base de données en ligne fonctionnant dans les environnements Windows, telles que Microsoft SQL, Microsoft Exchange, SAPR/3 et Oracle, ou fonctionnant dans les environnements UNIX, telles que SAP R/3, Oracle et Informix.
- Un système d'aide en ligne dynamique et contextuel appelé le "navigateur de l'aide".

Figure 1-13 Interface graphique utilisateur de Data Protector



Présentation des tâches nécessaires à la configuration de Data Protector

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

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

   Vous pouvez également utiliser Data Protector à l'aide d'un mot de passe temporaire. Celui-ci n'est cependant valable que pendant 60 jours à compter de la date d'installation. Pour plus d'informations à ce sujet, reportez-vous au *Guide d'installation et de choix des licences HP OpenView Storage Data Protector*.
5. Tenez compte des aspects ayant trait à la sécurité :
   - Analysez les questions liées à la sécurité : Reportez-vous au *Guide d'installation et de choix des licences HP OpenView Storage Data Protector*.
   - Tenez compte des groupes d'utilisateurs à configurer.

6. Décidez quelle devra être la structure de vos sauvegardes :
   - Quels pools de supports seront utilisés et de quelle manière ?
   - Quels périphériques seront utilisés et de quelle manière ?
   - Combien de copies de chaque sauvegarde souhaitez-vous ?
   - De combien de spécifications de sauvegarde avez-vous besoin et comment ces dernières devront-elles être regroupées ?
7. Installez et configurez votre environnement Data Protector.
   - Installez le système du Gestionnaire de cellule Data Protector et utilisez l'interface utilisateur de Data Protector pour distribuer les composants Data Protector sur d'autres systèmes.
   - Connectez les périphériques (lecteurs de bande) aux systèmes qui devront les contrôler.
   - Configurez les périphériques de sauvegarde.
   - Configurez les pools de supports et préparez les supports.
   - Configurez les spécifications de sauvegarde, notamment la sauvegarde de l'IDB.
   - Le cas échéant, configurez les rapports.
8. Familiarisez-vous avec les tâches suivantes :
   - Gestion des échecs de sauvegarde
   - Comment effectuer les opérations de restauration
   - Duplication des données sauvegardées et mise au coffre des supports
   - Préparation de la récupération après sinistre
   - Gestion de la base IDB

2 Planification de la stratégie de sauvegarde

Description du chapitre

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

Il s'organise comme suit :

Planification d'une stratégie de sauvegarde

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

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

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

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

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

Définition des besoins relatifs à une stratégie de sauvegarde

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

- Quelle sont les **stratégies** de votre entreprise en matière de sauvegarde et de restauration ?

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

- Quels types de données sauvegarder ?

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

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

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

  Le temps de récupération correspond essentiellement au temps nécessaire pour accéder au support et pour procéder à la restauration des données sur les disques. La récupération d'un système complet demande plus de temps, car des étapes supplémentaires sont nécessaires. Pour plus d'informations, reportez-vous à la section "Récupération après sinistre" à la page 110.

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

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

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

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

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

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

- Quel volume de données sauvegarder ?

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

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

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

- Combien de temps peut prendre une sauvegarde ?

  Estimez le temps nécessaire à chaque sauvegarde. Ce paramètre a une incidence directe sur la durée pendant laquelle les données sont disponibles à l'utilisation. Les fichiers utilisateur peuvent être sauvegardés à tout moment, dès lors que les utilisateurs n'ont pas besoin d'y accéder. La disponibilité de certaines bases de données transactionnelles pour la sauvegarde peut, quant à elle, être limitée à quelques heures seulement. Le temps nécessaire à la sauvegarde dépend du type de sauvegarde effectuée (complète ou incrémentale). Pour en savoir plus, reportez-vous à la section "Sauvegardes complètes et incrémentales" à la page 68. Data Protector permet également de sauvegarder certaines applications courantes de base de données en ligne. Pour plus d'informations, reportez-vous au *Guide d'intégration de HP OpenView Storage Data Protector*.

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

De même, si la quantité d'informations à sauvegarder est conséquente et que le temps imparti est limité, songez à effectuer une sauvegarde directe afin de profiter de la vitesse SAN, du trafic réseau réduit et de l'absence de goulet d'étranglement du serveur de sauvegarde.

- A quelle fréquence sauvegarder les données ?

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

Facteurs influant sur votre stratégie de sauvegarde

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

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

Préparation d'un plan de stratégie de sauvegarde

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

- Définition de l'importance de la disponibilité (et de la sauvegarde) du système pour l'entreprise
  - — Nécessité de conserver les données sauvegardées à un emplacement distant en cas de sinistre
  - — Niveau de continuité des opérations

    Cela comprend notamment un plan de récupération et de restauration pour l'ensemble des systèmes client stratégiques.

— Sécurité des données sauvegardées

Nécessité de contrôler l'accès aux locaux, afin d'en interdire l'entrée à toute personne non autorisée. Cela comprend également la protection des données pertinentes contre tout accès non autorisé, à l'aide de dispositifs physiques et d'une protection électronique par mot de passe.

- Types de données à sauvegarder

  Déterminez les différents types de données utilisés par votre entreprise et la manière dont vous souhaitez les combiner dans les spécifications de sauvegarde, ainsi que leurs périodes de disponibilité respectives pour les sauvegardes. Vous pouvez regrouper les données en catégories, telles que Données commerciales, Données de ressources de l'entreprise, Données de projet et Données personnelles, chacune de ces catégories ayant des besoins spécifiques.

- Mise en œuvre de la stratégie de sauvegarde :

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

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

  — Comment regrouper les systèmes client dans des spécifications de sauvegarde ?

  Etudiez la meilleure manière de regrouper les spécifications de sauvegarde (par service, type de données ou fréquence de sauvegarde).

  — Comment planifier les sauvegardes ?

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

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

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

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

- Configuration des périphériques

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

  Si vous devez sauvegarder de grandes quantités de données, pensez à utiliser un périphérique de bibliothèques.

  Si vous avez de grandes quantités de données à sauvegarder ou si vous estimez que votre réseau va nuire à la vitesse de sauvegarde, songez à configurer votre système pour une sauvegarde directe en reliant un périphérique de bibliothèques au réseau SAN à l'aide d'une passerelle Fibre Channel.

- Gestion des supports

  Déterminez le type de support à utiliser, ainsi que la manière de regrouper les supports en pools et de placer les objets sur ces supports.

  Déterminez le mode d'utilisation des supports dans le cadre des stratégies de sauvegarde.

- Mise au coffre

  Déterminez si les supports doivent être stockés dans un lieu sûr (un coffre) où ils seront conservés durant une période déterminée. Dans cette optique, songez à dupliquer les données sauvegardées pendant ou après la sauvegarde.

- Administrateurs et opérateurs de sauvegarde

  Déterminez les droits des utilisateurs chargés d'administrer et d'utiliser votre produit de stockage.

Planification de cellules

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

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

Une ou plusieurs cellules ?

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

- Problèmes liés à l'administration des sauvegardes

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

- Taille des cellules

  La taille d'une cellule Data Protector a une influence sur les performances de la sauvegarde et sur la capacité à gérer la cellule. La taille maximale recommandée pour une cellule Data Protector est de 100 systèmes client. Les cellules comportant plus de 200 systèmes client sont moins faciles à gérer.

- A propos du réseau

  Pour des performances optimales, l'ensemble des systèmes client d'une cellule doit se trouver sur le même réseau local. Reportez-vous aux sections suivantes pour plus d'informations sur les autres points à prendre en considération concernant le réseau, notamment la configuration réseau.

- Emplacement géographique

  Si les systèmes client à sauvegarder se trouvent sur des sites séparés géographiquement, il peut être difficile de les gérer à partir d'une seule cellule et des problèmes réseau peuvent se produire entre les systèmes client. En outre, la sécurité des données peut poser problème.

- Fuseaux horaires

  Chaque cellule doit se trouver dans un fuseau horaire donné.

- Sécurité des données

  Dans Data Protector, la sécurité des données est définie au niveau de chaque cellule. Tout le travail d'administration de Data Protector s'effectue dans le cadre d'une seule cellule : les supports, les périphériques de sauvegarde et les données sauvegardées appartiennent à une seule cellule. Notez que Data Protector vous permet de partager des périphériques ou de déplacer des supports entre plusieurs cellules ; l'accès physique aux supports doit donc être sécurisé et limité au seul personnel autorisé.

- Environnements mixtes

  Data Protector vous permet de sauvegarder dans une même cellule des systèmes client de plates-formes différentes. Toutefois, il peut être pratique de regrouper dans une cellule les systèmes client partageant une même plate-forme. Par exemple, les systèmes client Windows peuvent être regroupés dans une cellule et les clients UNIX dans une autre. Cela est particulièrement utile si vous avez défini des stratégies et des administrateurs distincts pour chacun des environnements UNIX et Windows.

- Services et sites

  Vous pouvez regrouper chaque service ou site dans une cellule propre, par exemple en définissant une cellule pour le service comptabilité, une pour le service informatique et une autre pour le service

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

Installation et maintenance des systèmes client

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

Serveur d'installation et Gestionnaire de cellule

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

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

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

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

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

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

Création de cellules dans l'environnement UNIX

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

Création de cellules dans l'environnement Windows

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

Domaines Windows

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

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

La mise en correspondance d'une cellule Data Protector dans un domaine Windows permet également de simplifier le processus d'administration au sein de Data Protector lui-même. Pour cela, distribuez le logiciel de manière à ce que tous les systèmes client puissent être installés à l'aide d'un compte Windows central dans une organisation par domaine.

Toutefois, les autres opérations ne sont pas limitées à une organisation par domaine Windows, car toutes les opérations et vérifications de sécurité sont réalisées par le protocole interne de Data Protector et non par le dispositif de sécurité de Windows.

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

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

Groupes de travail Windows

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

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

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

Création de cellules dans un environnement mixte

Si vous travaillez dans un environnement mixte, nous vous recommandons de tenir compte des facteurs décrits au Chapitre , "Création de cellules dans l'environnement UNIX" à la page 39. Plus un environnement comporte de domaines et de groupes de travail, plus le nombre de comptes à créer et d'étapes à suivre est important pour distribuer le logiciel et préparer l'environnement à l'administration.

Cellules distantes géographiquement

Data Protector vous permet d'administrer facilement les cellules géographiquement distantes. Pour plus d'informations, reportez-vous à la section "Séparation d'un environnement en plusieurs cellules" à la page 16.

A propos des cellules géographiquement distantes

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

- Les données ne sont pas envoyées via un WAN.

  Les périphériques et les systèmes client que vous sauvegardez sont configurés localement.

- Les cellules sont configurées dans un MoM.

  Pour gérer de manière centralisée les cellules distantes géographiquement, vous devez les configurer dans un environnement MoM.

- Analysez les configurations utilisateur.

  Vous devez prendre en compte tous les points que nous avons mentionnés au sujet des configurations à domaine unique, à domaines multiples et par groupe de travail.

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

Environnement MoM

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

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

Analyse et planification des performances

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

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

Infrastructure

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

Sauvegarde locale ou réseau

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

Flux de données réseau Du disque vers la mémoire du système source, vers le réseau, vers la mémoire du système de destination, vers le périphérique

Flux de données local Du disque vers la mémoire vers le périphérique

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

Sauvegarde directe ou réseau/serveur

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

Flux de données réseau

Du disque vers la mémoire du système source, vers le réseau, vers la mémoire du système de destination, vers le périphérique

Flux de données direct

Du disque vers le périphérique

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

Périphériques

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

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

Matériel hautes performances autre que les périphériques

Performances des systèmes informatiques

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

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

Utilisation en parallèle du matériel

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

Quand utiliser le parallélisme ?

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

  Cette option permet à Data Protector de déterminer de manière dynamique les périphériques sur lesquels les objets (disques) doivent être sauvegardés. Activez cette fonctionnalité, en particulier lorsque vous devez sauvegarder un grand nombre de systèmes de fichiers dans un environnement dynamique.

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

Configuration des sauvegardes et des restaurations

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

Compression logicielle

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

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

Compression matérielle

La compression matérielle s'effectue comme suit : un périphérique reçoit les données d'origine d'un serveur de lecteurs et les écrit sur des supports en mode compressé. Ce procédé permet d'augmenter la vitesse à laquelle un lecteur de bande reçoit les données car le volume de données écrit sur la bande est moins important.

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

Sauvegardes complètes et incrémentales

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

Sauvegarde d'image disque ou sauvegarde de système de fichiers

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

Distribution des objets sur les supports

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

- Un objet (disque) est stocké sur un support.

  L'avantage de cette méthode est qu'il existe une relation fixe connue entre un objet et un support, sur lequel l'objet réside. Cela peut être utile pour le processus de restauration car le système a ainsi besoin d'accéder à *un seul* support.

  Toutefois, cette méthode présente un inconvénient dans une configuration de sauvegarde en réseau. En effet, le réseau agit comme un facteur de limitation des performances du système, empêchant le périphérique de fonctionner en mode continu.
- De nombreux objets sont stockés sur un petit nombre de supports ; chaque support contient des données provenant de plusieurs objets ; un objet est stocké sur un périphérique.

  L'avantage de cette méthode tient à la flexibilité des flux de données au moment de la sauvegarde, ce qui participe à l'optimisation des performances, en particulier dans le cas d'une configuration en réseau.

  La stratégie présuppose que les périphériques, à chacun desquels parviennent simultanément des données émanant de plusieurs sources, reçoivent un flux de données suffisant pour fonctionner en mode continu.

  L'inconvénient de cette méthode tient à la perte de temps résultant du fait que les données (d'autres objets) sont ignorées lors de la restauration d'un objet spécifique. En outre, cette méthode ne permet pas de prévoir précisément sur quel support seront stockées les données d'un objet.

  Pour plus d'informations sur le mode de fonctionnement continu des périphériques et les sauvegardes simultanées, reportez-vous à la section “Périphérique en mode continu et simultanéité” à la page 162.

Performances des disques

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

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

Fragmentation des disques

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

CONSEIL

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

Compression

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

Sauvegardes d'image disque

Data Protector vous permet également de sauvegarder des disques UNIX sous forme d'images disque. Avec une sauvegarde par image disque, une image de l'ensemble du disque est sauvegardée, sans suivre la structure du système de fichiers. La tête de disque se déplace de manière linéaire sur toute la surface du disque. La sauvegarde d'image disque peut donc s'effectuer beaucoup plus rapidement que celle d'un système de fichiers.

Performances SAN

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

Performances des applications de base de données en ligne

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

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

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

Planification de la sécurité

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

Qu'est-ce que la sécurité ?

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

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

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

Fonctionnalités de sécurité Data Protector

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

- Cellules
- Comptes utilisateur Data Protector
- Groupe d'utilisateurs Data Protector
- Droits utilisateur Data Protector
- Visibilité et accès aux données sauvegardées

Cellules

Démarrage de sessions

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

Manager-of-Managers de Data Protector. De cette manière, les utilisateurs d'autres cellules ne peuvent ni sauvegarder, ni restaurer les données stockées dans les systèmes de votre cellule locale.

Accès à partir d'un Gestionnaire de cellule spécifique

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

Restriction pré- et post-exécution

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

Comptes utilisateur Data Protector

Compte utilisateur Data Protector

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

Qui définit les comptes utilisateur ?

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

A quel moment les comptes sont-ils contrôlés ?

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

Pour plus d'informations, reportez-vous au Chapitre 4, "Utilisateurs et groupes d'utilisateurs" à la page 195.

Groupes d'utilisateurs Data Protector

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

Lorsqu'un compte d'utilisateur est créé, l'utilisateur devient membre du groupe d'utilisateurs spécifié. Pour chaque groupe, des droits utilisateur Data Protector spécifiques ont été définis. Tous les membres du groupe disposent des droits définis pour le groupe.

A quoi servent les groupes d'utilisateurs ?

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

Pour plus d'informations, reportez-vous au Chapitre 4, "Utilisateurs et groupes d'utilisateurs" à la page 195.

Droits utilisateur Data Protector

Que sont les droits utilisateur ?

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

A quoi servent les droits utilisateur ?

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

Pour plus d'informations, reportez-vous au Chapitre 4, "Utilisateurs et groupes d'utilisateurs" à la page 195.

Visibilité des données sauvegardées

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

Interdiction d'accès aux données pour d'autres utilisateurs

Lorsque vous configurez une sauvegarde, vous devez décider si les données seront visibles par tous les utilisateurs (publiques) ou uniquement par le propriétaire de la sauvegarde (privées) au moment de la restauration. Le propriétaire est l'utilisateur qui a configuré la sauvegarde et lancé (planifié) la session de sauvegarde. Pour plus d'informations sur les propriétaires de sauvegarde, reportez-vous à la section "Qui est propriétaire d'une session de sauvegarde ?" à la page 53.

Encodage des données

Les systèmes ouverts et l'utilisation de réseaux publics rendent la protection des données indispensable au sein des grandes entreprises. Data Protector vous permet d'encoder les données stockées dans les systèmes de fichiers et dans les images disque afin de les rendre illisibles. L'encodage des données a lieu avant leur transfert sur un réseau et avant leur écriture sur des supports. Pour encoder les données, Data Protector utilise un algorithme intégré fixe.

Qui est propriétaire d'une session de sauvegarde ?

Qu'est-ce que la propriété de sauvegarde ?

Par défaut, l'utilisateur Data Protector qui a créé une spécification de sauvegarde devient propriétaire de la session de sauvegarde en cours et du jeu de supports qui en résulte. Notez que cette notion de propriété fait référence à l'utilisateur Data Protector et non à l'utilisateur du système (plate-forme). La session de sauvegarde ne s'exécute donc pas sous le nom d'utilisateur du propriétaire.

Qui peut démarrer une sauvegarde ?

Vous ne pouvez exécuter que les spécifications de sauvegarde que vous avez créées. Par conséquent, si une spécification de sauvegarde a été créée par l'administrateur, les autres utilisateurs ne sont pas autorisés à démarrer de sauvegarde pour cette spécification. Reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector* pour savoir comment changer le propriétaire d'une sauvegarde. Notez que le changement de propriétaire d'une sauvegarde revient à autoriser une personne à accéder/restaurer des données dont elle n'est pas forcément propriétaire.

Propriété et restauration des sauvegardes

La notion de propriété a également une influence sur votre capacité à restaurer les données. Si l'option privé/public est définie sur privé, seul le propriétaire du jeu de supports ou les administrateurs sont autorisés à voir les données stockées dans le jeu.

Gestion de clusters

Concepts relatifs aux clusters

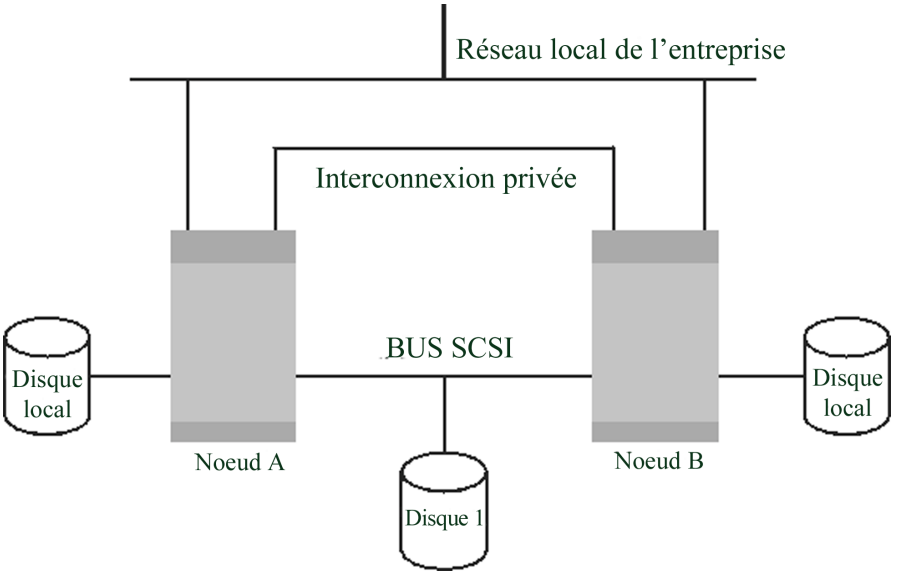
Qu'est-ce qu'un cluster ?

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

- Garantir une disponibilité des applications et ressources stratégiques aussi élevée que possible.
- Tolérer les pannes de composant.
- Prendre en charge l'ajout et le retrait de composants.

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

Figure 2-1 Structure d'un cluster type



Composants :

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

Nœuds de cluster

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

Disques partagés

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

Réseau de cluster

Un réseau de cluster est un réseau privé qui relie tous les nœuds de cluster. Il transfère les données internes du cluster appelées **pulsation du cluster**. La pulsation est un paquet de données comportant un

horodatage, distribué à tous les nœuds de cluster. Les nœuds de cluster, en comparant ces paquets, déterminent celui d'entre eux qui est toujours opérationnel, ce qui leur permet de déterminer l'appartenance du **package** (MC/SG, Veritas Cluster) ou du **groupe** (MSCS).

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

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

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

Qu'est-ce qu'un serveur virtuel ?

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

Qu'est-ce qu'un basculement ?

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

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

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

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

Haute disponibilité du Gestionnaire de cellule Data Protector

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

Redémarrage automatique des sauvegardes

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

Partage de charge en cas de basculement

Un utilitaire spécial par ligne de commande permet aux utilisateurs d'effectuer différentes opérations, et notamment l'abandon des sessions de sauvegarde au cas où des applications non Data Protector basculeraient. Le Gestionnaire de cellule Data Protector permet à l'administrateur de définir les opérations à exécuter dans ce type de situation. Si la sauvegarde a moins d'importance que l'application, Data Protector peut abandonner les sessions en cours. Si la sauvegarde est plus importante ou sur le point de se terminer, Data Protector peut poursuivre les sessions. Reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector* pour plus d'informations sur la procédure de définition des critères.

Support de clusters

Le support de clusters Data Protector signifie que :

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

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

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

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

- Le redémarrage complet.
- Le redémarrage des objets ayant échoué.
- Pas de redémarrage.

Reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector* pour obtenir plus d'informations sur les options de comportement de la session de sauvegarde du Gestionnaire de cellule Data Protector.

Exemples d'environnements de clusters

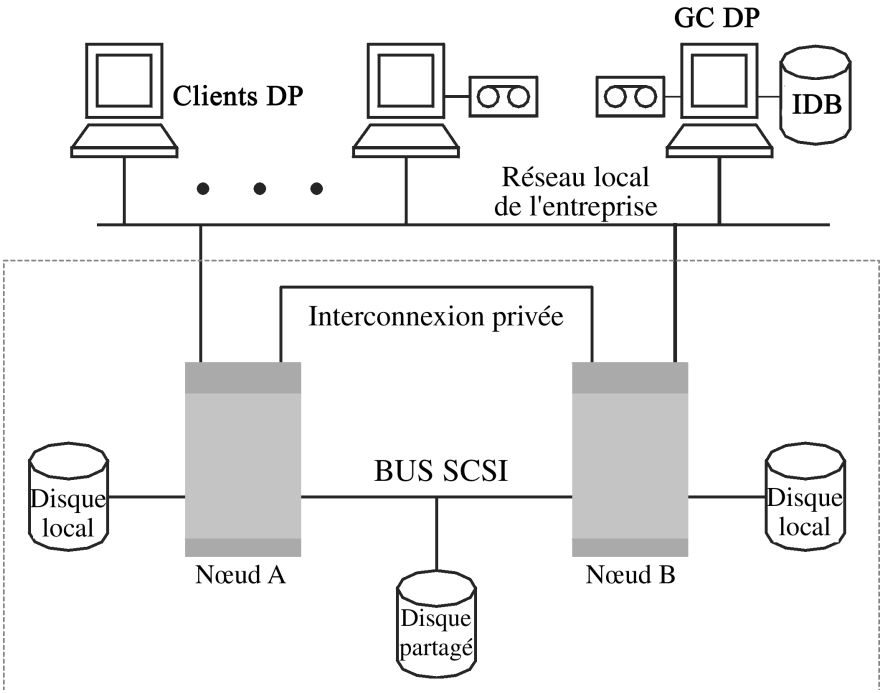
Vous trouverez dans cette section trois exemples de configurations de cluster.

Gestionnaire de cellule installé hors d'un cluster

L'environnement est le suivant :

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

Figure 2-2 **Gestionnaire de cellule installé hors d'un cluster**



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

- Nœud physique A
- Nœud physique B
- Serveur virtuel

Sauvegarde du serveur virtuel

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

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

Tableau 2-1 Comportement de la sauvegarde

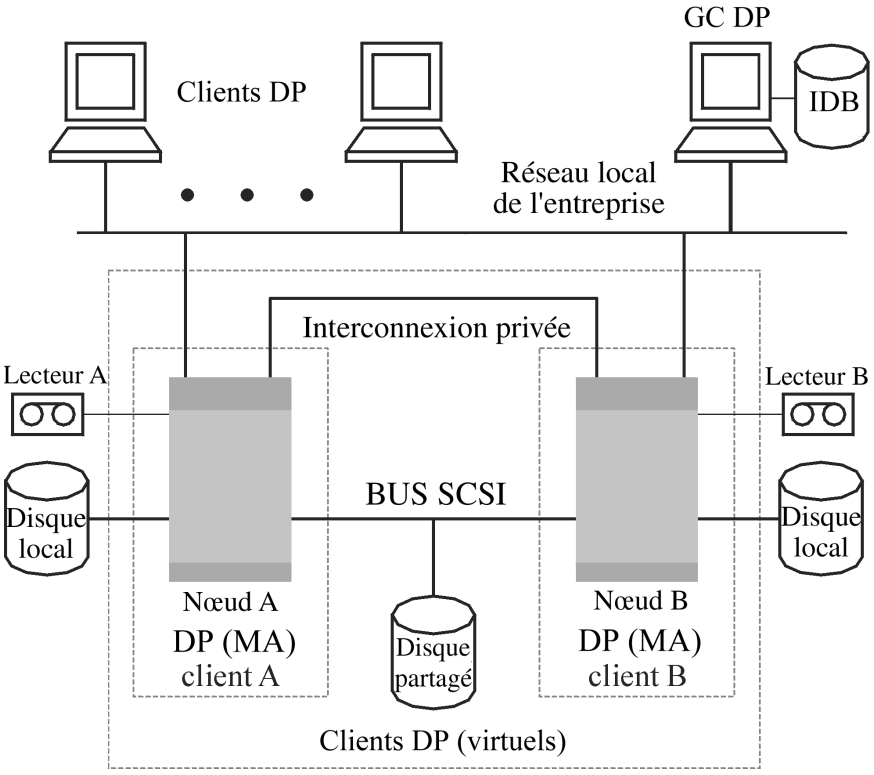
Condition	Résultat
Basculement du nœud avant le démarrage de la sauvegarde	Sauvegarde réussie
Basculement du nœud pendant la sauvegarde	**Sauvegarde d'image disque/de système de fichiers :** Echec de la session de sauvegarde. Les objets entièrement sauvegardés peuvent être utilisés pour effectuer les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

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

L'environnement est le suivant :

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

Figure 2-3 **Gestionnaire de cellule installé hors d'un cluster, périphériques connectés aux nœuds de cluster**



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

- Nœud physique A
- Nœud physique B
- Serveur virtuel

Sauvegarde du serveur virtuel

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

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

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

Tableau 2-2 Comportement de la sauvegarde

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

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

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

L'environnement est le suivant :

- Le Gestionnaire de cellule est installé dans un cluster.

  En ce qui concerne les intégrations de l'application Data Protector, il existe deux façons de configurer Data Protector ainsi qu'une application dans une telle configuration :

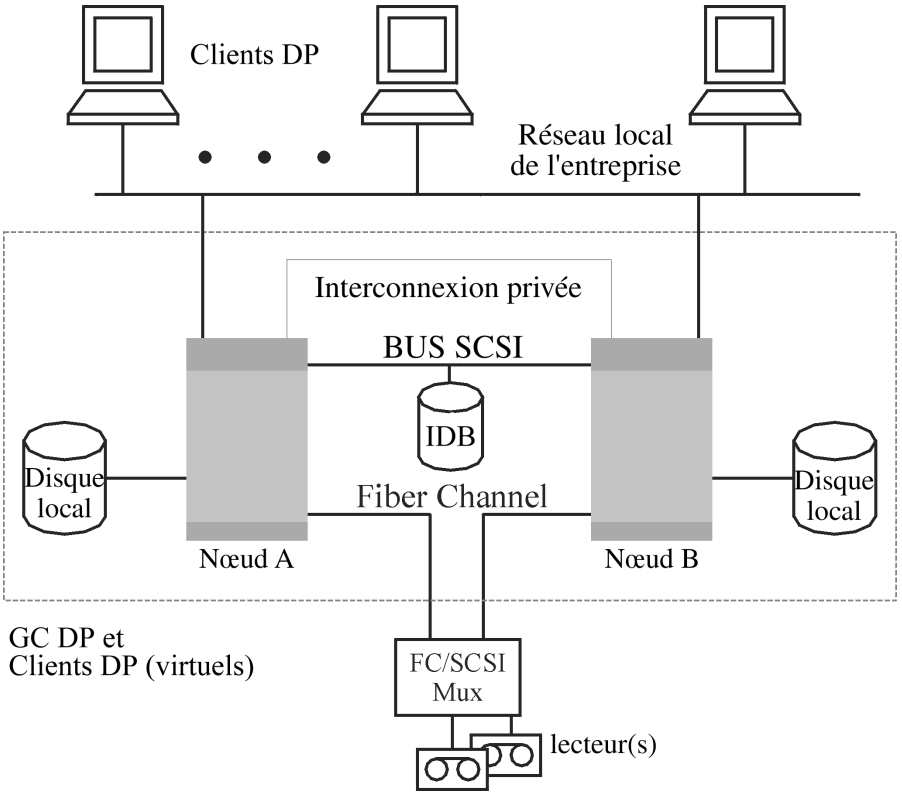
  — Le Gestionnaire de cellule Data Protector est configuré pour s'exécuter (à la fois en exécution normale et lors du basculement) sur le même nœud que l'application. Les ressources critiques de cluster Data Protector sont définies dans le même package (MC/ServiceGuard) ou groupe (Microsoft Cluster Server) que les ressources critiques de cluster de l'application.

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

  — Le Gestionnaire de cellule Data Protector est configuré pour s'exécuter (à la fois en exécution normale et lors du basculement) sur des nœuds autres que celui de l'application. Les ressources critiques de cluster Data Protector sont définies dans un autre package (MC/ServiceGuard) ou groupe (Microsoft Cluster Server) que les ressources critiques de cluster de l'application.

- Le(s) périphérique(s) de sauvegarde sont connectés au bus Fibre Channel partagé du cluster via un multiplexeur FC/SCSI.

Figure 2-4 **Gestionnaire de cellule installé dans le cluster, périphériques connectés aux nœuds de cluster**



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

- Nœud physique A
- Nœud physique B
- Serveur virtuel

Sauvegarde du serveur virtuel

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

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

Dans cette configuration, vous pouvez accéder aux fonctions suivantes :

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

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

- Contrôle des charges système au moment du basculement.

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

  — Si la sauvegarde a moins d'importance que l'application qui vient de basculer vers le système de sauvegarde, Data Protector peut abandonner les sessions en cours.

  — Si elle a plus d'importance ou qu'elle est sur le point d'être effectuée, Data Protector poursuit les sessions.

Reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector* pour plus d'informations sur la procédure de définition de ces options.

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

Tableau 2-3 Comportement de la sauvegarde

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

Tableau 2-3 Comportement de la sauvegarde

<table>
<tr><th>Condition</th><th colspan="2">Résultat</th></tr>
<tr><td rowspan="2">Basculement de l'application et du Gestionnaire de cellule pendant la sauvegarde (le Gestionnaire de cellule s'exécute sur le même nœud que l'application).</td><td>Sauvegarde d'image disque/de système de fichiers :
Echec de la session de sauvegarde. Les objets entièrement sauvegardés peuvent être utilisés pour effectuer des restaurations. Par contre, les objets dont la sauvegarde a échoué (en cours d'exécution ou en attente) doivent être sauvegardés à nouveau en redémarrant manuellement la session.</td><td rowspan="2">IMPORTANT
Pour redémarrer la session, il est important de sélectionner l'option appropriée dans Data Protector. Reportez-vous au Guide de l'administrateur de HP OpenView Storage Data Protector pour obtenir des informations sur la définitions de toutes actions possibles de Data Protector en cas de basculement du Gestionnaire de cellule.</td></tr>
<tr><td>Sauvegarde d'application :
Echec de la session de sauvegarde. Cette session est redémarrée automatiquement.</td></tr>
<tr><td rowspan="2">Basculement de l'application pendant la sauvegarde sans basculement du Gestionnaire de cellule (ce dernier s'exécute sur un nœud autre que celui de l'application).</td><td colspan="2">Sauvegarde d'image disque/de système de fichiers :
La session de sauvegarde échoue lors du basculement du nœud sur lequel le système de fichiers est installé. Les objets entièrement sauvegardés peuvent être utilisés pour effectuer les restaurations. Par contre, les objets ayant échoué (en cours d'exécution ou en attente) doivent être sauvegardés à nouveau en redémarrant manuellement la session.</td></tr>
<tr><td colspan="2">Sauvegarde d'application :
Echec de la session de sauvegarde. La session doit être redémarrée manuellement.</td></tr>
</table>

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

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

Sauvegardes complètes et incrémentales

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

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

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

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

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

Sauvegardes complètes

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

Avantages des sauvegardes complètes

Les sauvegardes complètes présentent les avantages suivants :

- Elles permettent d'accélérer et de simplifier la restauration de manière significative. Pour récupérer la dernière version de vos fichiers, vous n'avez besoin que des supports de la dernière sauvegarde complète.
- Elles sont plus fiables. Toutes les données sont sauvegardées en une seule session de sauvegarde et leur restauration est assez simple.

Inconvénients des sauvegardes complètes

Les sauvegardes complètes présentent les inconvénients suivants :

- Elles sont plus longues à réaliser.
- La même version d'un fichier est sauvegardée plusieurs fois et occupe donc davantage d'espace sur les supports et dans la base de données IDB.

Sauvegardes incrémentales

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

Avant d'effectuer une sauvegarde incrémentale d'un objet sauvegarde spécifique, Data Protector compare les arborescences de l'objet sauvegarde à celles de la chaîne de restauration valide de l'objet de sauvegarde en question. Une chaîne de restauration valide comprend la dernière sauvegarde complète protégée et toutes les sauvegardes incrémentales (éventuelles) suivantes du même objet sauvegarde, ainsi que les mêmes arborescences spécifiées. Si les arborescences ne concordent pas (par exemple, les arborescences de l'objet sauvegarde ne sont plus les mêmes) ou s'il existe plusieurs spécifications de sauvegarde avec le même objet de sauvegarde et différentes arborescences spécifiées, une sauvegarde complète est effectuée automatiquement à la place de la sauvegarde incrémentale. Il convient de s'assurer que tous les fichiers ayant été modifiés depuis la dernière sauvegarde sont sauvegardés.

Avantages des sauvegardes incrémentales

Les sauvegardes incrémentales présentent les avantages suivants :

- Elles occupent moins d'espace sur les supports.
- Elles occupent moins d'espace dans la base de données IDB.
- Elles sont moins longues à réaliser car les quantités de données sauvegardées sont moins importantes.

Inconvénients des sauvegardes incrémentales

Les sauvegardes incrémentales présentent les inconvénients suivants :

- La restauration est plus longue, car les données doivent être restaurées à partir de la sauvegarde complète la plus récente et de toutes les sauvegardes incrémentales qui ont suivi jusqu'à la date spécifiée.
- La restauration nécessite donc un nombre de supports plus important, car il se peut que la sauvegarde complète et les sauvegardes incrémentales ultérieures aient été stockées sur des supports différents.

  Pour plus d'informations, reportez-vous à la section "Sélection des supports utilisés pour la sauvegarde" à la page 151.

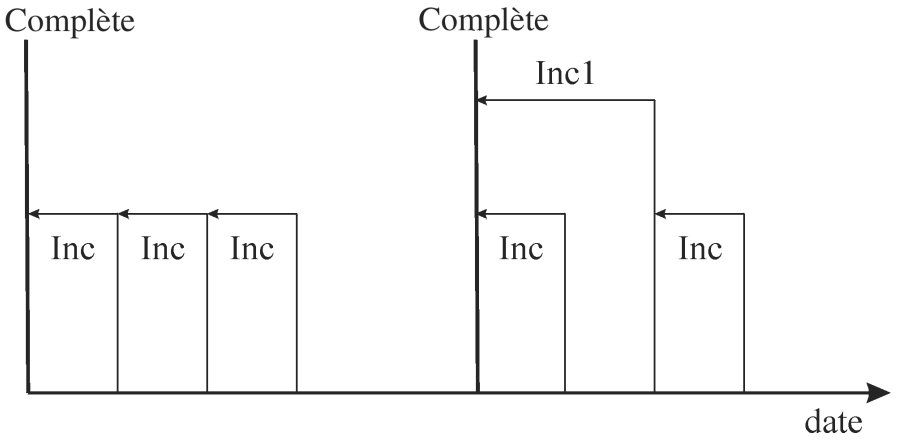
  Pour plus d'informations sur les autres facteurs qui influent sur la restauration, reportez-vous à la section "Observations relatives à la restauration" à la page 72.

Types de sauvegardes incrémentales

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

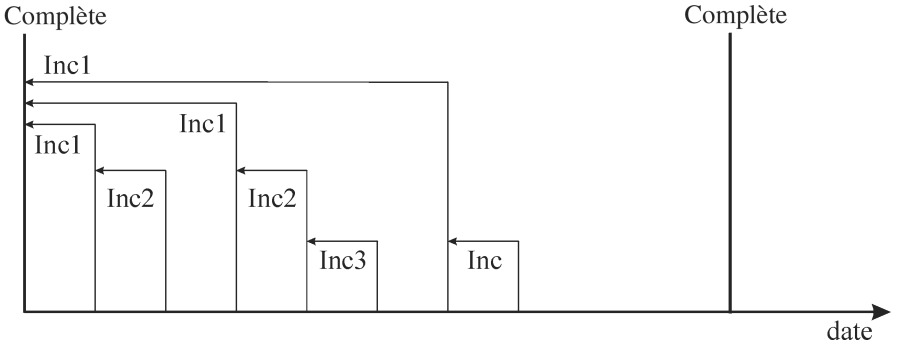
Incr	Ce type de sauvegarde (voir figure 2-5) est basé sur une sauvegarde préalable *quelconque* encore sous protection, qu'elle soit complète ou incrémentale. Ce type de sauvegarde est également appelé **sauvegarde différentielle** car seules les modifications effectuées depuis la sauvegarde précédente sont prises en compte.
Incr1-9	Une **sauvegarde incrémentale par niveau** (voir figure 2-6) dépend de la dernière sauvegarde en date du niveau immédiatement inférieur, dont les données sont toujours protégées. Exemple : une sauvegarde Incr1 consiste à sauvegarder toutes les modifications effectuées depuis la sauvegarde complète la plus récente, tandis qu'une sauvegarde Incr5 consiste à sauvegarder toutes les modifications effectuées depuis la sauvegarde de type Incr4 la plus récente. Une sauvegarde Incr1-9 ne fait *jamais* référence à une sauvegarde Incr existante.

Figure 2-5 **Sauvegardes différentielles**



La figure 2-5 et la figure 2-6 illustrent différents types de sauvegardes incrémentales. Les sauvegardes incrémentales dépendent de la dernière sauvegarde complète effectuée. A chaque démarrage de sauvegarde incrémentale, Data Protector vérifie s'il existe une sauvegarde complète protégée des données sauvegardées. Si aucune sauvegarde complète protégée n'est définie, Data Protector lance une sauvegarde complète à la place.

Figure 2-6 **Sauvegardes incrémentales par niveau**



Observations relatives à la restauration

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

Jeux de supports

L'utilisation des sauvegardes différentielles et incrémentales par niveau (voir figure 2-7) requiert l'accès aux cinq **jeux de supports** les plus récents, jusqu'à la sauvegarde complète incluse. L'espace nécessaire sur les supports est moins important dans ce cas, mais la restauration quelque peu complexe. La série de jeux de supports requis est également appelée **chaîne de sauvegarde**.

CONSEIL

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

Une autre utilisation courante du concept de sauvegarde incrémentale est illustrée à la figure 2-8. Dans ce cas, l'espace nécessaire sur les supports est légèrement plus important. Vous avez besoin d'accéder à deux jeux de supports uniquement pour procéder à la restauration des données à un instant donné. Notez qu'il n'existe aucune dépendance avec un jeu de supports Incr1 précédent éventuel pour cette restauration, sauf si vous déplacez l'instant donné pour la restauration en question.

Figure 2-7 **Supports nécessaires à la restauration à partir de sauvegardes différentielles et de sauvegardes par niveau**

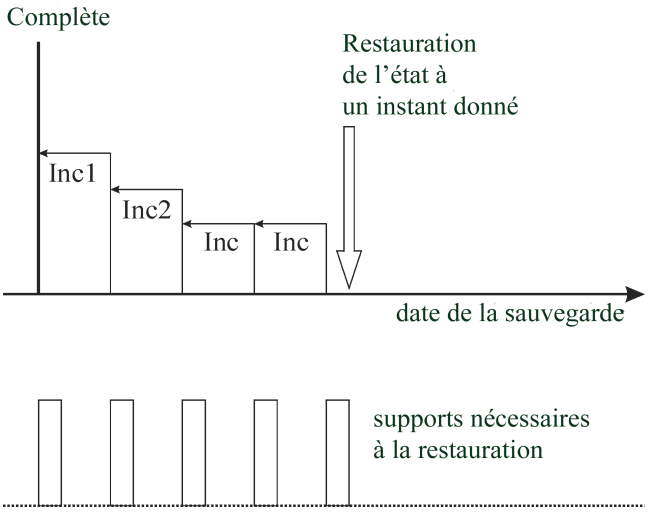
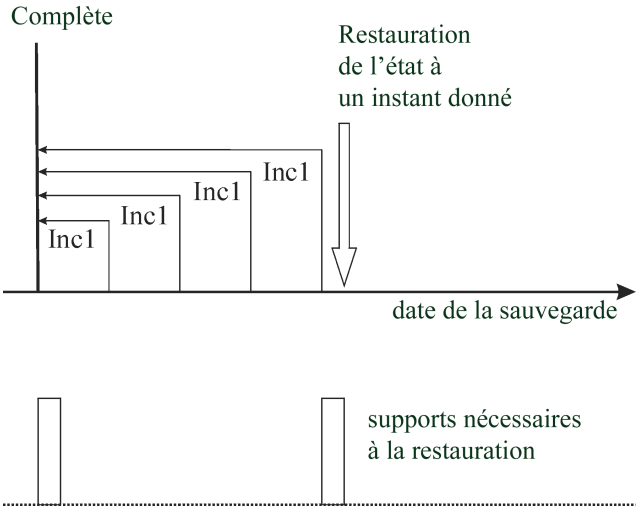


Figure 2-8 **Supports nécessaires à la restauration à partir de sauvegardes incrémentales par niveau**



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

n'est pas correctement définie, il est possible que la chaîne de sauvegarde soit rompue. Pour plus d'informations, reportez-vous au Annexe B.

Planification et types de sauvegarde

Vous avez la possibilité de combiner des sauvegardes complètes et incrémentales lorsque vous configurez des sauvegardes planifiées sans surveillance. Vous pouvez, par exemple, réaliser une sauvegarde complète le dimanche, puis des sauvegardes incrémentales tous les jours ouvrables de la semaine. Pour sauvegarder une grande quantité de données et éviter des flux de données trop importants, nous vous recommandons d'utiliser la méthode de la planification échelonnée. Reportez-vous à l'"Planification répartie de sauvegardes complètes" à la page 86. Pour plus d'informations sur la procédure de planification efficace de vos sauvegardes, reportez-vous également à la section "Types de sauvegarde et sauvegardes planifiées" à la page 83.

Conservation des données sauvegardées et des informations sur les données

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

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

Base de données interne de Data Protector

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

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

Protection de données

Qu'est-ce que la protection des données ?

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

Différentes parties de Data Protector vous permettent de définir la protection des données. Pour plus de détails, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

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

Protection de catalogue

Qu'est-ce que la protection de catalogue ?

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

Cette protection peut être définie en dates absolues ou relatives.

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

Pour obtenir des informations supplémentaires sur la manière dont la protection de catalogue influe sur les performances et la croissance de l'IDB, reportez-vous à la section "Protection de catalogue en tant que paramètre clé réglable de l'IDB" à la page 220.

Le modèle de protection utilisé par Data Protector peut être mis en correspondance avec le concept de génération de sauvegarde présenté à la section “Informations supplémentaires” à la page B-1.

Niveau de journalisation

Qu’est-ce que le niveau de journalisation ?

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

Data Protector propose quatre niveaux de journalisation permettant de contrôler la quantité de détails sur les fichiers et répertoires écrits dans l’IDB. Pour plus d’informations, reportez-vous à la section “Niveau de journalisation en tant que paramètre clé réglable de la base de données IDB” à la page 218.

Exploration des fichiers à restaurer

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

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

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

Activation de l’exploration des fichiers et de la restauration rapide

Pour pouvoir restaurer des fichiers rapidement, les informations sur les données sauvegardées doivent exister dans le catalogue tout comme les données protégées sur le support. Les informations du catalogue vous permettent de parcourir et de sélectionner des fichiers, et de démarrer

leur restauration à l'aide de l'interface utilisateur de Data Protector ; elles permettent également à Data Protector de localiser rapidement les données sur les supports de sauvegarde.

Activation de la restauration des fichiers, sans l'exploration

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

Ecrasement des fichiers sauvegardés par de nouvelles données

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

CONSEIL

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

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

Exportation de supports d'une cellule

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

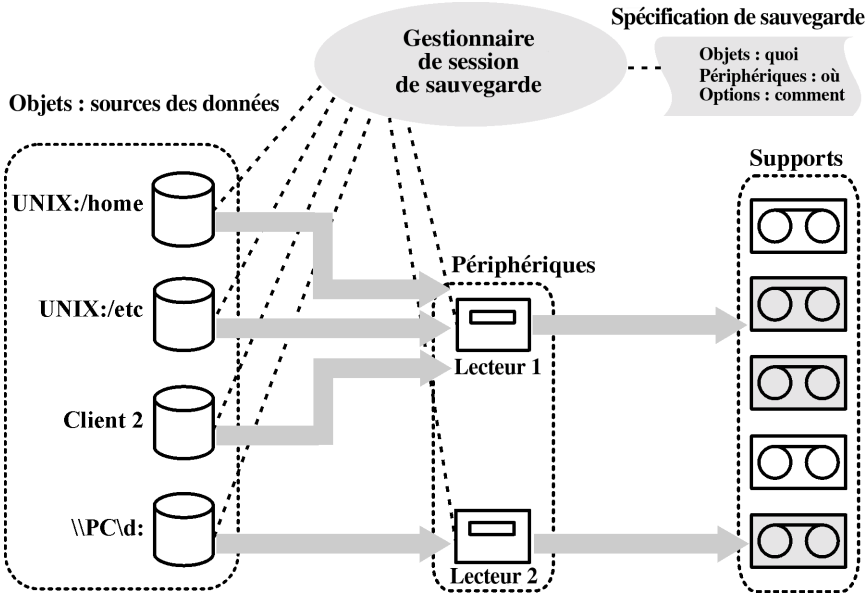
Sauvegarde de données

La sauvegarde de données comporte plusieurs étapes :

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

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

Figure 2-9 Session de sauvegarde



A l'heure spécifiée, Data Protector démarre une session de sauvegarde sur la base d'une spécification de sauvegarde. La source de données est définie sous forme d'une liste d'objets (comme un système de fichiers

sous UNIX ou des lecteurs de disque sous Windows) et les destinations sont des périphériques (à bandes par exemple) spécifiés. Au cours de la session de sauvegarde, Data Protector lit le contenu des objets, transfère les données via le réseau et les écrit sur les supports placés dans les périphériques. Le nom des périphériques à utiliser figure dans la spécification de sauvegarde. Un pool de supports peut également y être spécifié. Dans le cas contraire, le pool par défaut est utilisé.

Une spécification de sauvegarde peut être une simple définition de la sauvegarde d'un disque sur un lecteur DDS autonome, ou une définition complexe de la sauvegarde de 40 serveurs volumineux sur une bibliothèque à bandes Silo comportant huit lecteurs.

Création d'une spécification de sauvegarde

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

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

Comment créer une spécification de sauvegarde ?

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

Data Protector vous permet de sauvegarder un client avec l'ensemble des disques qui y sont connectés, en détectant ces derniers au moment de la sauvegarde. Reportez-vous à la section "Sauvegarde en mode détection de disques" à la page 261.

Sélection d'objets sauvegarde

Qu'est-ce qu'un objet sauvegarde ?

Data Protector utilise le terme **objet sauvegarde** pour désigner une unité de sauvegarde contenant tous les éléments sélectionnés pour réaliser une sauvegarde à partir d'un volume de disque (disque logique ou point de montage). Les éléments sélectionnés peuvent être des

fichiers, des répertoires ou l'ensemble du disque ou du point de montage. En outre, un objet sauvegarde peut être une entité de base de données ou une image disque (rawdisk).

Un objet sauvegarde est défini comme suit :

- Nom de client : nom d'hôte du client Data Protector dans lequel l'objet sauvegarde est hébergé.
- Point de montage : point d'accès dans une structure de répertoires (lecteur sous Windows et point de montage sous UNIX) sur le client contenant l'objet sauvegarde.
- Description: définit exclusivement les objets sauvegarde avec un nom de client et un point de montage identiques.
- Saisissez : type d'objet sauvegarde, par exemple, un système de fichier ou Oracle.

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

Exemples d'options de sauvegarde

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

- Niveau de journalisation des informations destinées à la base de données IDB

  Data Protector propose quatre niveaux de journalisation permettant de contrôler la quantité de détails concernant les fichiers et répertoires stockés dans la base de données IDB :

  — Journaliser tout

  — Fichiers journaux

  — Journaliser répertoires

  — Pas de journalisation

Notez que lorsque vous changez le niveau des informations stockées, les possibilités d'exploration des fichiers via l'interface Data Protector durant la restauration s'en trouvent affectées. Pour plus d'informations sur le niveau de journalisation, reportez-vous à la section "Niveau de journalisation en tant que paramètre clé réglable de la base de données IDB" à la page 218.

- Partage de charge automatique

  Allocation de périphérique dynamique à partir d'une liste donnée.

  Cette option permet à Data Protector de déterminer de manière dynamique les périphériques sur lesquels les objets (disques) doivent être sauvegardés.

- Scripts pré-exécution et post-exécution

  Traitement destiné à préparer un client à une sauvegarde cohérente. Pour plus d'informations, reportez-vous à la section "Commandes pré-exécution et post-exécution" à la page 259.

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

Sessions de sauvegarde

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

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

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

Reportez-vous au Chapitre 7, "Fonctionnement de Data Protector" à la page 253 pour obtenir des informations détaillées sur les sessions de sauvegarde et sur la manière de les contrôler.

Miroirs d'objet

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

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

Pour plus d'informations, reportez-vous à la section "Mise en miroir d'objet" à la page 101.

Jeux de supports

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

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

Types de sauvegarde et sauvegardes planifiées

Une stratégie de planification permet de déterminer à quel moment démarrent les sauvegardes et de définir le type de sauvegarde effectuée (complète ou incrémentale).

Avant de choisir le type de sauvegarde, nous vous recommandons de prendre en compte les points suivants :

Types de sauvegarde

- Les sauvegardes complètes sont plus longues à réaliser que les sauvegardes incrémentales et requièrent un espace plus important sur les 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.

- Les sauvegardes complètes permettent d'effectuer de manière simple et rapide des restaurations, sans avoir à fournir de supports pour chaque sauvegarde incrémentale.
- Durant les sauvegardes complètes, un plus grand nombre d'informations sur les données sauvegardées est enregistré dans la base de données catalogue, ce qui contribue à accroître plus rapidement la taille de la base.
- Les sauvegardes incrémentales tiennent compte uniquement des modifications de votre environnement et seules les modifications effectuées depuis la sauvegarde la plus récente sont prises en compte. Cela a pour conséquence d'accélérer considérablement la vitesse de sauvegarde, mais peut diminuer les performances de restauration.

Planification, configurations et sessions de sauvegarde

Configuration de sauvegarde

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

Pour chaque sauvegarde individuelle ou périodique, vous pouvez spécifier les options suivantes : `Type de sauvegarde` (complète ou incrémentale), `Charge réseau` et `Protection de sauvegarde`. Avec la sauvegarde Split Mirror/Snapshot, dans le cas d'une sauvegarde sur disque ou d'une ZDB sur disque + bande (restauration instantanée activée), choisissez l'option `Sauvegarde Split Mirror/Snapshot`. Pour ces sauvegardes, le type de la sauvegarde est ignoré et l'opération réalisée est une sauvegarde complète.

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

Session de sauvegarde

Au démarrage d'une session de sauvegarde, Data Protector tente d'allouer toutes les ressources nécessaires, telles que les périphériques. La session reste en file d'attente tant que les ressources minimales requises ne sont pas disponibles. Data Protector tente d'allouer les

ressources pendant une période spécifique : le délai d'attente. Vous pouvez configurer ce dernier. Si les ressources ne sont toujours pas disponibles au terme du délai d'attente, la session est abandonnée.

Optimisation des performances de sauvegarde

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

Planification - Conseils et pièges à éviter

Les concepts de génération de sauvegarde, de protection de données et de protection de catalogue sont décrits dans les sections "Sauvegardes complètes et incrémentales" à la page 68 et "Conservation des données sauvegardées et des informations sur les données" à la page 75.

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

Quand planifier des sauvegardes ?

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

Pensez à planifier les sauvegardes complètes des différents clients (spécifications de sauvegarde) sur plusieurs jours, comme indiqué à la section "Planification répartie de sauvegardes complètes".

REMARQUE

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

Planification répartie de sauvegardes complètes

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

Tableau 2-4 Méthode de planification échelonnée

	Lun	Mar	Mer	...
grp_système_a	COMPL.	Incr1	Incr1	...
grp_système_b	Incr1	COMPL.	Incr1	...
grp_système_c	Incr1	Incr1	COMPL.	...

Optimisation de la restauration

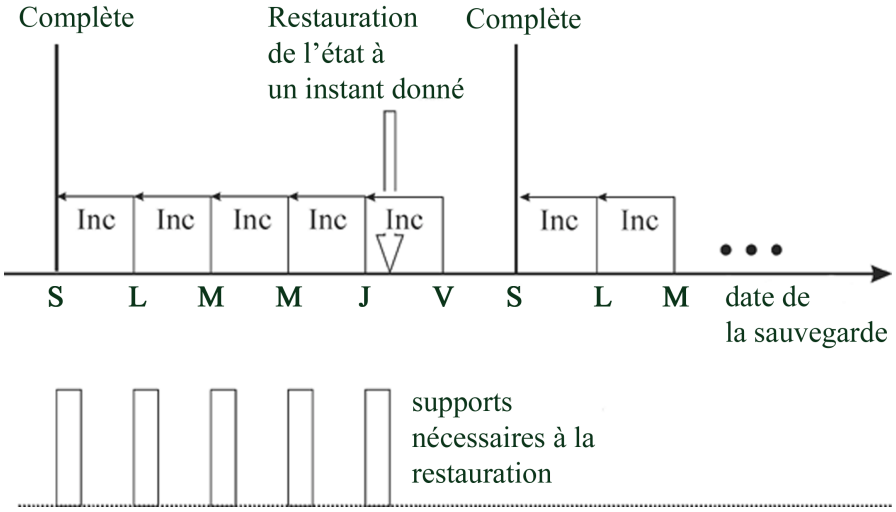
La combinaison de votre stratégie de planification avec des sauvegardes complètes ou incrémentales a une grande incidence sur le temps nécessaire à la restauration des données. Trois exemples sont fournis dans cette section à titre d'illustration.

Pour pouvoir effectuer une restauration de l'état à un instant donné, vous devez disposer d'une sauvegarde complète, ainsi que de toutes les sauvegardes incrémentales réalisées entre cette dernière et l'instant en question. Les sauvegardes complètes et incrémentales n'étant généralement pas effectuées sur les mêmes supports, vous devrez probablement charger différents supports. Pour obtenir des informations complémentaires sur la manière dont Data Protector sélectionne les supports pour les sauvegardes, reportez-vous à la section “Sélection des supports utilisés pour la sauvegarde” à la page 151.

Exemple 1

La figure 2-10 illustre une stratégie de planification basée sur une sauvegarde complète associée à des sauvegardes différentielles.

Figure 2-10 **Sauvegarde complète avec sauvegardes différentielles quotidiennes**

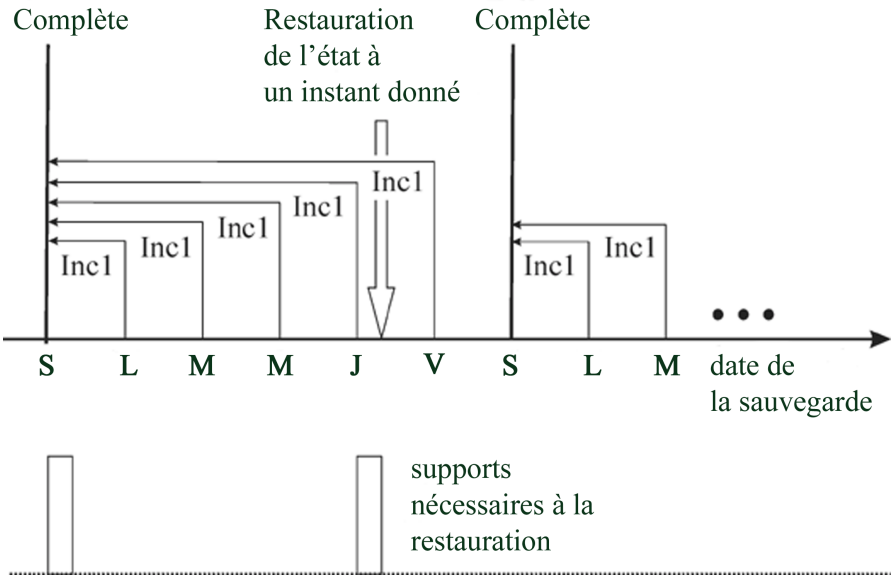


Cette stratégie permet de réduire l'espace support et le temps nécessaires aux sauvegardes, car seules les modifications effectuées depuis la veille sont prises en compte. Toutefois, pour restaurer des fichiers sauvegardés un jeudi, par exemple, vous aurez besoin des supports utilisés pour la sauvegarde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

Exemple 2

La figure 2-11 illustre une stratégie de planification basée sur une sauvegarde complète associée à des sauvegardes incrémentales de niveau un.

Figure 2-11 **Sauvegarde complète avec sauvegardes incrémentales de niveau 1 quotidiennes**

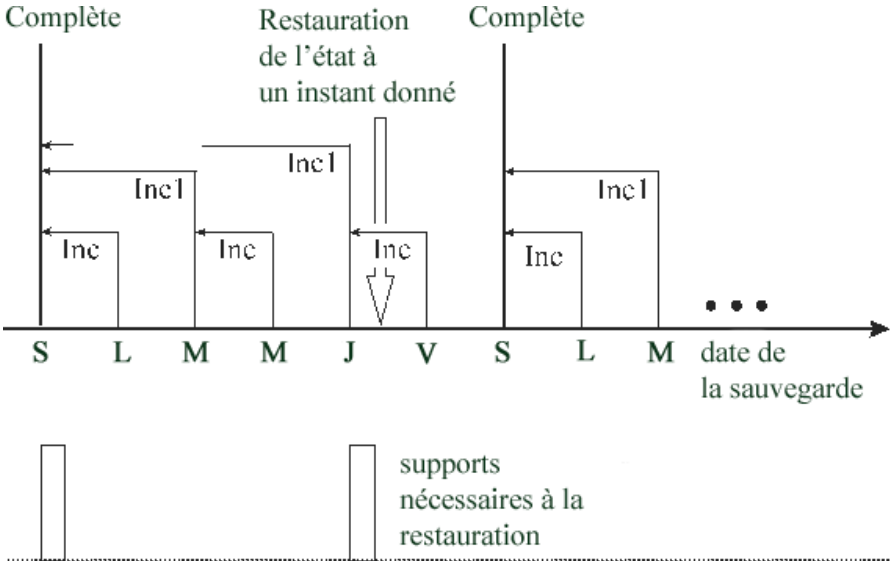


Cette stratégie nécessite légèrement plus de temps pour les sauvegardes et requiert un peu plus d'espace support, puisque toutes les modifications effectuées depuis la sauvegarde complète la plus récente sont enregistrées chaque jour. Pour restaurer des fichiers sauvegardés un jeudi, par exemple, vous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

Exemple 3

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

Figure 2-12 **Sauvegarde complète avec sauvegardes incrémentales mixtes**



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

Des opérations automatisées ou sans surveillance

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

A propos des sauvegardes sans surveillance

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

- A quel moment l'utilisation du système et l'activité des utilisateurs sont-elles les plus faibles ?

  C'est généralement pendant la nuit, et c'est à ce moment-là qu'est planifiée l'exécution de la plupart des sauvegardes. Data Protector peut générer des rapports sur les périphériques utilisés pour les sauvegardes.

- De quel type sont les données à traiter et à quelle fréquence souhaitez-vous planifier leur sauvegarde ?

  Les données souvent modifiées et stratégiques pour l'entreprise, telles que les fichiers utilisateur, les transactions et les bases de données, doivent être sauvegardées régulièrement. A l'inverse, il n'est pas nécessaire de sauvegarder souvent les données spécifiques au système, comme les fichiers de programme, qui sont peu susceptibles d'être modifiées.

- Jusqu'à quel point souhaitez-vous simplifier la restauration ?

  Selon la manière dont vous planifiez vos sauvegardes complètes et incrémentales, vous aurez besoin des supports utilisés lors des différentes sauvegardes pour pouvoir restaurer la version la plus récente des fichiers. La procédure peut prendre plus ou moins de temps, voire nécessiter un traitement manuel des supports si vous ne disposez pas d'un périphérique de bibliothèque automatique.

- Quelle quantité de données devez-vous sauvegarder ?

  Les sauvegardes complètes sont plus longues à réaliser que les sauvegardes incrémentales. Les sauvegardes doivent généralement être effectuées dans un intervalle de temps limité.

- Combien de supports sont requis ?

  Définissez une stratégie de rotation des supports. Reportez-vous à la section "Mise en œuvre d'une stratégie de rotation des supports" à la page 146. Vous saurez ainsi si le nombre de supports pouvant être conservés dans la bibliothèque prévue est suffisant pour effectuer des sauvegardes sur la période définie sans devoir gérer les supports manuellement.

- Comment traiter les invites de montage ?

  Déterminez si vous avez besoin d'utiliser une ou plusieurs bibliothèques. Si vous n'en utilisez qu'une, Data Protector peut alors accéder à la quasi-totalité des supports, ce qui signifie qu'il peut fonctionner en mode automatique, réduisant ainsi de manière significative les interventions manuelles sur les supports. Si le volume de données à traiter est trop important pour une seule bibliothèque, envisagez d'utiliser plusieurs bibliothèques. Pour plus d'informations, reportez-vous au "Grandes bibliothèques" à la page 170.

- Comment gérer les périphériques non disponibles ?

  Utilisez les fonctions d'équilibrage dynamique des charges, ou chaînage des périphériques, et pensez à définir plusieurs périphériques lors de la création d'une spécification de sauvegarde. Vous éviterez ainsi l'échec d'une sauvegarde dans le cas où un périphérique ne serait pas prêt ou en cas de dysfonctionnement du système auquel le périphérique est connecté.

- Combien de temps peut prendre une sauvegarde de l'ensemble des données ?

  Les sauvegardes devant être effectuées pendant les périodes où l'utilisation du réseau et l'activité des utilisateurs sont faibles, il est indispensable de planifier les sauvegardes de manière à distribuer la charge réseau qui en résulte et à optimiser l'efficacité des sessions de sauvegarde. Vous serez peut-être amené à mettre en place une stratégie de planification échelonnée.

- Comment préparer les applications en cours d'exécution pour les sauvegardes ?

  Bon nombre d'applications laissent des fichiers ouverts, de sorte que l'exécution d'une sauvegarde aboutirait à des incohérences. Pour remédier à cela, utilisez les scripts pré- et post-exécution qui permettront de synchroniser l'état des applications avec les opérations de sauvegarde.

Duplication de données sauvegardées

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

Data Protector fournit les méthodes suivantes de duplication des données sauvegardées : copie d'objet, mise en miroir d'objet et copie de support. Reportez-vous au tableau 2-5 pour une vue d'ensemble des principales caractéristiques de ces méthodes.

Tableau 2-5 Méthodes de duplication de données Data Protector

	Copie d'objet	**Mise en miroir d'objet**	**Copie de supports**
Eléments dupliqués	Toute combinaison de versions d'objet d'une ou plusieurs sessions de sauvegarde	Un ensemble d'objets d'une session de sauvegarde	Un support dans son intégralité
Temps de duplication	A tout moment à l'issue d'une sauvegarde	Pendant la sauvegarde	A tout moment à l'issue d'une sauvegarde
Type de support source et cible	Peut différer	Peut différer	Doit être identique
Taille des supports source et cible	Peut différer	Peut différer	Doit être identique
Ajout de supports cible	Oui	Oui	Non[a]

Tableau 2-5 Méthodes de duplication de données Data Protector

	Copie d'objet	Mise en miroir d'objet	Copie de supports
Résultat de l'opération	Supports contenant les versions d'objet sélectionnées	Supports contenant les versions d'objet sélectionnées	Supports identiques aux supports source

a. Vous ne pouvez utiliser comme supports cible que des supports non formatés, vierges ou dont la protection est expirée. Après l'opération, aucun ajout n'est possible aux supports source et cible.

Copie d'objets

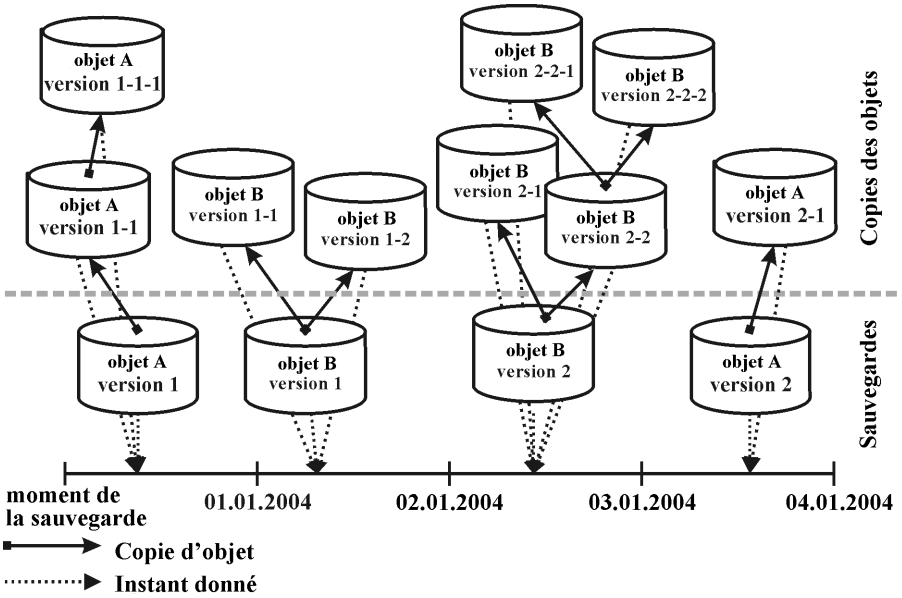
Qu'est-ce que la copie d'objet ?

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

Le résultat d'une session de copie d'objet est un ensemble de supports contenant des copies des versions d'objet que vous avez spécifiées.

La figure 2-13 à la page 95 indique comment les données sauvegardées à un moment donné peuvent être copiées ultérieurement. Vous pouvez copier un objet sauvegarde à partir d'un support contenant une sauvegarde ou d'un support contenant une copie de l'objet.

Figure 2-13 Concept de la copie d'objet



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

Début de la session de copie d'objet

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

Copie d'objet après sauvegarde

La copie d'objet après sauvegarde intervient après la fin d'une session de sauvegarde définie dans la spécification de copie d'objet automatisée. Elle permet de copier les objets sélectionnés en fonction de la spécification de copie d'objet automatisée et ayant été sauvegardés au cours de cette session de sauvegarde particulière.

Copie d'objet planifiée

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

Sélection des périphériques

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

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

Si vous ne spécifiez pas les périphériques source à utiliser dans la spécification de copie d'objet Data Protector utilise les périphériques par défaut. Par défaut, les périphériques utilisés pour l'écriture des objets serviront de périphériques source. Si les périphériques de destination ne sont pas spécifiés par objet, Data Protector les sélectionne automatiquement parmi ceux que vous avez choisis dans la spécification de copie d'objet, en fonction des critères suivants et par ordre de priorité :

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

Les périphériques sont verrouillés au début de la session. Les périphériques non disponibles à ce moment-là ne pourront pas être utilisés pendant la session puisque le verrouillage des périphériques ne peut pas être effectué une fois la session commencée. Si une erreur survient au niveau du support, le périphérique concerné ne doit pas être utilisé pendant la session de copie.

Sélection du jeu de supports depuis lequel effectuer la copie

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

Le processus global de sélection des supports est le même que pour la restauration. Pour plus d'informations, reportez-vous à la section "Sélection du jeu de supports" à la page 107.

Performances d'une session de copie d'objet

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

Pourquoi utiliser la copie d'objet ?

D'autres copies des données sauvegardées sont créées à des fins diverses et variées :

- Mise au coffre

  Vous pouvez faire des copies d'objets sauvegardés et les stocker à plusieurs emplacements.
- Libération de supports

  Pour conserver uniquement les versions d'objet protégées sur les supports, vous pouvez copier ces versions d'objet et les écraser sur le support.
- Démultiplexage des supports

  Vous pouvez copier des objets pour éliminer l'entrelacement des données.
- Regroupement d'une chaîne de restauration

  Vous pouvez copier toutes les versions d'objet nécessaires pour une restauration vers un seul jeu de supports.
- Migration vers un autre type de support

  Vous pouvez copier vos sauvegardes sur des supports de différents types.
- Prise en charge des concepts de sauvegarde avancés

  Vous pouvez utiliser des concepts de sauvegarde tels que la sauvegarde de disque en plusieurs étapes.

Mise au coffre

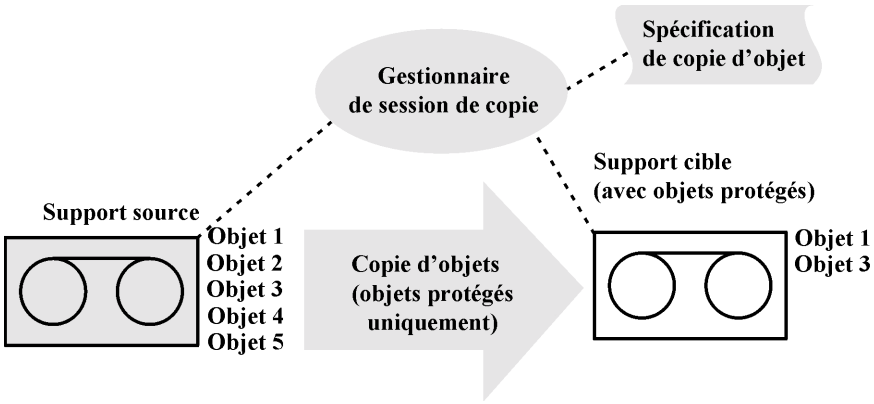
La mise au coffre est un processus de stockage des supports dans un lieu sûr, souvent appelé coffre, où ils peuvent être conservés pendant une période donnée. Pour plus de détails, reportez-vous à la section “Mise au coffre” à la page 156.

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

Libération de supports

Vous pouvez réduire le nombre de supports utilisés en conservant uniquement les sauvegardes protégées et en écrasant les autres. Un support pouvant contenir aussi bien des sauvegardes protégées que non protégées, vous pouvez copier des objets protégés sur un nouveau jeu de supports et écraser les autres. Consultez la figure 2-14 à la page 98.

Figure 2-14 Libération de supports

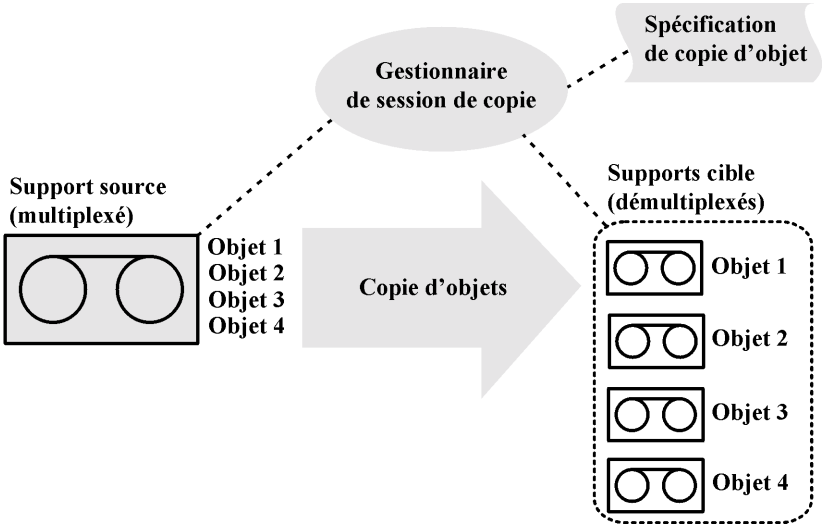


Démultiplexage des supports

Les supports multiplexés peuvent contenir des données entrelacées de plusieurs objets. Ces supports peuvent provenir de sessions de sauvegarde dont la simultanéité des périphériques est supérieure à 1. Les supports multiplexés compromettent la confidentialité des sauvegardes et la restauration est plus longue.

Data Protector permet de démultiplexer les supports. Les objets provenant d’un support multiplexé sont copiés sur les différents supports que vous spécifiez. Consultez la figure 2-15 à la page 99.

Figure 2-15 Démultiplexage d'un support



Regroupement d'une chaîne de restauration

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

Migration vers un autre type de support

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

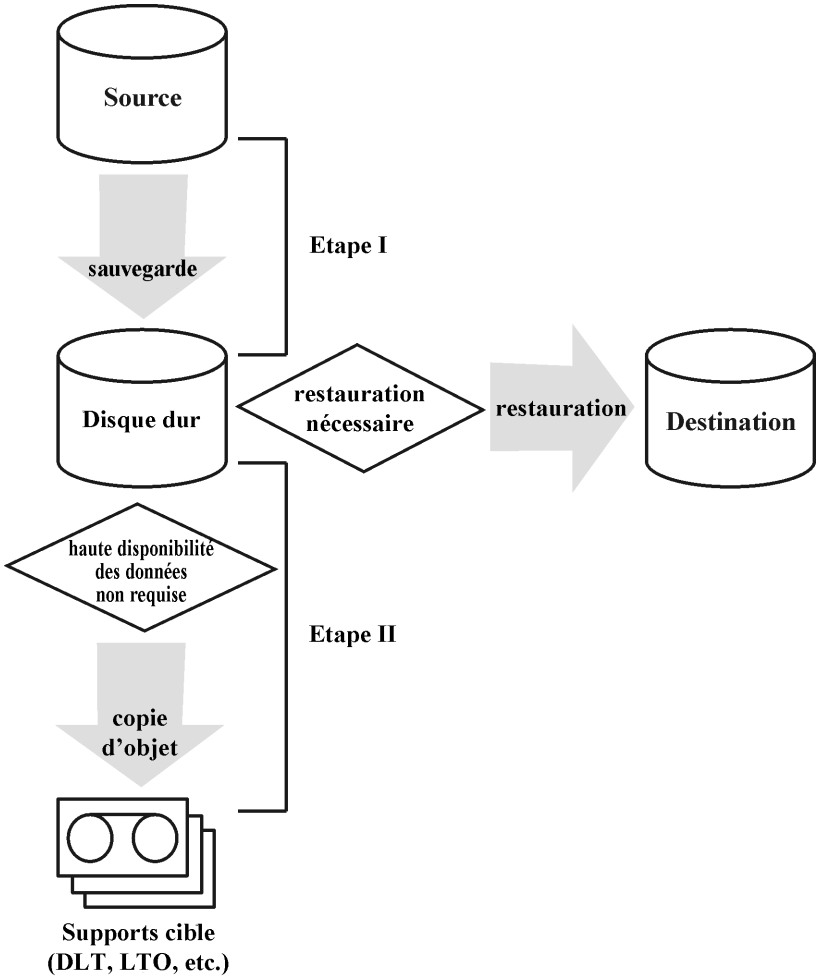
Sauvegarde de disque en plusieurs étapes

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

Les étapes de la sauvegarde consistent à sauvegarder des données sur des supports d'un certain type, puis à les déplacer vers des supports d'un type différent. Les données sont sauvegardées vers des supports caractérisés par de hautes performances et une grande accessibilité, mais par des capacités limitées (par exemple, des disques système).

Ces sauvegardes restent généralement accessibles à la restauration pendant la période où ce type d'opération est le plus probable. Après un certain temps, les données sont déplacées vers des supports dont les performances et l'accessibilité sont moins élevées mais dont les capacités de stockage sont importantes, au moyen de la fonction de copie d'objet. Consultez la figure 2-16 à la page 100.

Figure 2-16 Concept de sauvegarde de disque en plusieurs étapes



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

Mise en miroir d'objet

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

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

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

Avantages de la mise en miroir d'objet

L'utilisation de la mise en miroir d'objet répond aux objectifs suivants :

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

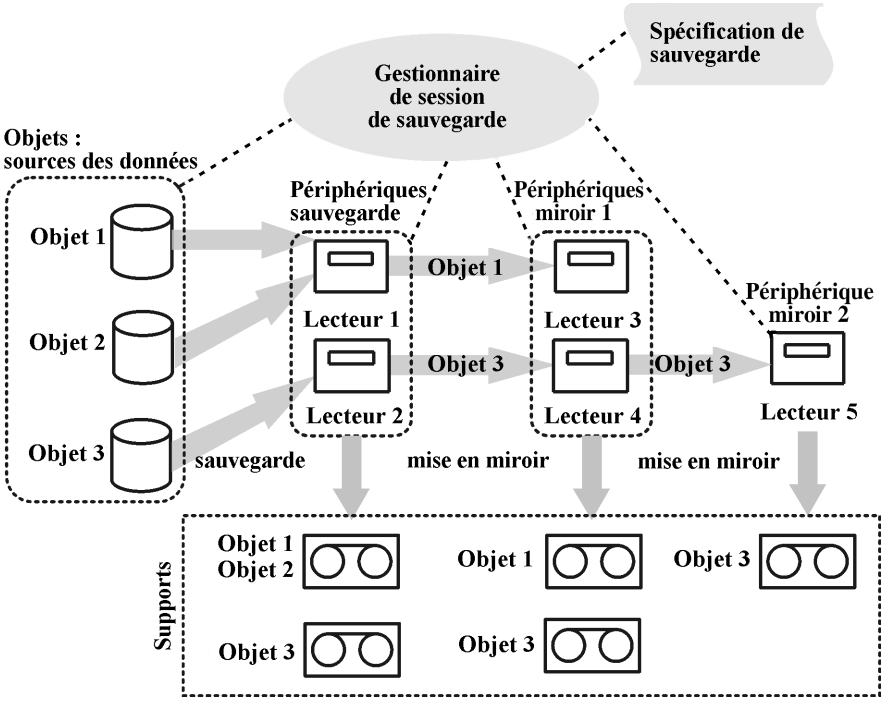
Opération de mise en miroir d'objet

Dans une session de sauvegarde avec mise en miroir d'objet, chaque objet sélectionné est sauvegardé et mis en miroir simultanément autant de fois que spécifié dans la spécification de sauvegarde. Consultez la figure 2-17 à la page 102.

Prenons comme exemple l'Objet 3 de la figure. L'Agent de disque lit un bloc de données à partir du disque et l'envoie vers l'Agent de support responsable de la sauvegarde de l'objet. L'Agent de support écrit les données sur le support du Lecteur 2 et les transmet à l'Agent de support responsable du miroir 1. Ce dernier écrit à son tour les données sur le

support du Lecteur 4 et les transmet à l'Agent de support responsable du miroir 2. Celui-ci écrit les données sur le support du Lecteur 5. A la fin de la session, l'Objet 3 est disponible sur trois supports.

Figure 2-17 Mise en miroir d'objet



Sélection des périphériques

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

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

Lorsque vous effectuez une mise en miroir d'objet à partir de la ligne de commande, le partage de charge n'est pas disponible.

Performances de sauvegarde

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

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

Les performances de sauvegarde dépendent également de facteurs tels que la taille de bloc et la connexion des périphériques. Si les périphériques utilisés pour la sauvegarde et la mise en miroir d'objet présentent des tailles de bloc différentes, les données mises en miroir seront regroupées pendant la session, ce qui demande plus de temps et monopolise plus de ressources. Si les données sont transférées via le réseau, cela implique une charge supplémentaire pour le réseau et une durée d'opération plus longue.

Copie de supports

Qu'est-ce que la copie de supports ?

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

Il est possible de copier des supports manuellement ou de configurer Data Protector pour que la copie soit effectuée automatiquement. Pour plus d'informations, reportez-vous à la section "Copie automatisée des supports" à la page 104.

Comment copier des supports ?

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

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

Quel est le résultat ?

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

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

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

Copie automatisée des supports

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

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

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

Copie de supports après sauvegarde

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

Copie de supports programmée

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

Comment fonctionne la copie automatisée des supports ?

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

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

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

Pour obtenir des exemples d’utilisation, reportez-vous à la section “Exemples de copie automatisée des supports” à la page B-5.

Restauration des données

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

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

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

Durée de la restauration

En cas de perte de données, l'accès aux données n'est possible qu'au terme du processus de récupération. Il est généralement crucial de réduire au minimum la durée de la restauration de manière à ce que les utilisateurs puissent travailler normalement. Il est par conséquent recommandé d'évaluer le temps nécessaire à la restauration de données spécifiques.

Facteurs ayant une influence sur la durée de la restauration

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

- La quantité de données à restaurer. Ce paramètre a une influence directe sur l'ensemble des éléments suivants.
- La combinaison de sauvegardes complètes et incrémentales choisie. Pour plus d'informations, reportez-vous au "Sauvegardes complètes et incrémentales" à la page 68.
- Les supports et les périphériques utilisés pour la sauvegarde. Pour plus d'informations, reportez-vous au Chapitre 3, "Gestion des supports et périphériques" à la page 133.

- La vitesse de fonctionnement des réseaux et systèmes. Pour plus d'informations, reportez-vous au "Analyse et planification des performances" à la page 43.
- L'application que vous voulez récupérer, par exemple, des fichiers de base de données Oracle. Pour obtenir des informations complémentaires, reportez-vous au *Guide d'intégration de HP OpenView Storage Data Protector* adéquat.
- L'utilisation de la restauration parallèle. Selon comment les données ont été sauvegardées, plusieurs objets peuvent être restaurés au moyen d'une seule opération de lecture. Reportez-vous à la section "Restaurations parallèles" à la page 268.
- Les paramètres de niveau de journalisation sélectionnés Reportez-vous à la section "Niveau de journalisation en tant que paramètre clé réglable de la base de données IDB" à la page 218.

Sélection du jeu de supports

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

Algorithme de sélection des jeux de supports

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

Priorité des emplacements des supports

Pour influer sur la sélection des jeux de supports, spécifiez la priorité des emplacements des supports. Il importe que vous utilisiez le concept de stockage sur plusieurs sites. Si vous conservez des supports sur plusieurs sites, vous pouvez spécifier l'emplacement le mieux adapté à une

restauration spécifique. Data Protector utilisera le jeu de supports dont la priorité est la plus élevée si plusieurs jeux de supports correspondent aux conditions de l'algorithme de sélection.

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

Opérateurs autorisés à restaurer les données

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

Quand utiliser cette stratégie ?

Vous pouvez recourir à cette stratégie dans les cas suivants :

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

Actions requises

Pour mettre en œuvre cette stratégie, procédez comme suit :

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

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

Utilisateurs finaux autorisés à restaurer les données

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

Quand utiliser cette stratégie ?

Vous pouvez recourir à cette stratégie dans les cas suivants :

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

Actions requises

Pour mettre en œuvre cette stratégie, procédez comme suit :

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

Récupération après sinistre

Cette section propose une présentation des méthodes de récupération après sinistre disponibles et inclut un tableau décrivant les combinaisons possibles de méthodes de récupération après sinistre et de systèmes d'exploitation. Utilisez le tableau pour naviguer dans le reste de ce chapitre.

Qu'est-ce qu'un sinistre informatique ?

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

Qu'est-ce que le système d'origine ?

Le **système d'origine** désigne la configuration système sauvegardée par Data Protector avant qu'un sinistre ne frappe le système.

Qu'est-ce qu'un système cible ?

Le système cible désigne le système une fois que le sinistre s'est produit. Il est généralement non amorçable et l'objet de la récupération après sinistre Data Protector consiste justement à redonner à ce système sa configuration initiale. La différence entre le système endommagé et le système cible réside dans le fait que, pour le système cible, le matériel défaillant a été remplacé.

Que sont les disques/partitions/volumes d'amorçage et disques/partitions/volumes système ?

Un(e) **disque/partition/volume d'amorçage** désigne le (la) disque/partition/volume contenant les fichiers requis pour assurer la première étape du processus d'amorçage, tandis que le (la) **disque/partition/volume système** désigne celui (celle) qui contient les fichiers du système d'exploitation.

REMARQUE Microsoft définit la partition d'amorçage comme la partition contenant les fichiers du système d'exploitation, et la partition système comme celle qui contient les fichiers requis pour assurer la première étape du processus d'amorçage.

Qu'est-ce qu'un système hôte ?

Le **système hôte** est un client Data Protector en fonctionnement utilisé pour la récupération après sinistre avec restitution de disque à l'aide d'un Agent de disque installé.

Qu'est-ce qu'un disque auxiliaire ?

Un disque auxiliaire est un disque amorçable doté d'un système d'exploitation minimal avec la gestion de réseau et un Agent de disque installés. Il peut être transporté et utilisé pour amorcer le système cible dans la première phase de la récupération après sinistre avec restitution de disque des clients UNIX.

Qu'est-ce qu'un système d'exploitation de récupération après sinistre (DR OS) ?

Le **système d'exploitation de récupération après sinistre (DR OS)** est un environnement de système d'exploitation dans lequel le processus de récupération après sinistre s'exécute. Il fournit à Data Protector un environnement d'exécution de base (accès aux disque, réseau, bande et système de fichiers). Il doit être installé et configuré pour que la récupération après sinistre Data Protector puisse être effectuée.

Le DR OS peut être temporaire ou actif. Le **DR OS temporaire** est utilisé uniquement en tant qu'environnement hôte pour la restauration d'un autre système d'exploitation et des données de configuration du système cible. Il est supprimé à l'issue de la restauration du système cible dans la configuration système d'origine. Le **DR OS actif** héberge non seulement le processus de récupération après sinistre Data Protector, mais fait également partie du système restauré car il remplace ses propres données de configuration par les données de configuration d'origine.

Que sont les volumes critiques ?

Les **volumes critiques** sont les volumes nécessaires à l'amorçage du système et des fichiers Data Protector. Quel que soit le système d'exploitation, ils incluent les éléments suivants :

- Volume d'amorçage.
- Volume système.
- Fichiers exécutables de Data Protector.
- Base de données IDB (Gestionnaire de cellule uniquement).

REMARQUE Tous les volumes sur lesquels réside la base de données IDB sont critiques.

Outre les volumes critiques cités ci-dessus, CONFIGURATION fait également partie du jeu de volumes critiques pour les systèmes Windows. Les services sont sauvegardés en tant que partie de la sauvegarde CONFIGURATION.

Certains éléments inclus dans une CONFIGURATION peuvent être placés sur des volumes autres que les volumes système, d'amorçage, Data Protector ou IDB. Dans ce cas, les volumes suivants font aussi partie du jeu de volumes critiques :

- Volume des profils d'utilisateur.
- Volume de la base de données Certificate Server.
- Volume du service Active Directory sur le contrôleur de domaine.
- Volume quorum sur Microsoft Cluster Server.

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

- Le système doit être rétabli à l'état en ligne aussi vite et efficacement que possible.
- Les administrateurs ne sont pas coutumiers de la procédure requise pour réaliser la récupération après sinistre.
- Il se peut également que le personnel chargé d'effectuer la récupération ne possède qu'une connaissance générale du système.

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

Processus de récupération

Le processus de récupération après sinistre est constitué de quatre phases, la *phase 0* (préparation) étant un prérequis à une récupération après sinistre réussie. Au cours de la *phase 1*, le DR OS est installé et configuré, ce qui implique généralement un repartitionnement et un reformatage de la partition d'amorçage ; en effet, la partition système ou d'amorçage du système n'est pas toujours disponible.

Or, l'environnement doit être rétabli avant de pouvoir poursuivre les opérations normales de restauration. Le système d'exploitation possédant toutes les informations de configuration et définissant l'environnement avec Data Protector (tel qu'il était) est restauré au cours de la *phase 2*. Ce n'est qu'après cette étape que la restauration des applications et des données utilisateur est possible (*phase 3*). Pour que la restauration soit aussi rapide et efficace que possible, il convient d'appliquer un processus en plusieurs étapes bien défini.

Cohérence et pertinence de la sauvegarde

Lorsqu'un sinistre se produit, le système cible doit être rétabli dans l'état où il se trouvait au moment de la sauvegarde. En outre, il doit être ramené au même état opérationnel et fonctionnel que celui dans lequel il se trouvait juste avant que la sauvegarde ne se fasse. Dans certaines circonstances, cela peut être particulièrement délicat. Certaines applications, même fermées, ne sont pas totalement inactives.

Sur les systèmes UNIX, des démons ou autres processus peuvent être activés dès la fin de l'amorçage du système, pour différentes raisons (par exemple sous HP-UX : le serveur de licence au niveau 2 d'exécution). Ce type de processus peut également lire les données stockées dans la mémoire et écrire un "indicateur de problème" dans un fichier lorsqu'il est en cours d'exécution. Une application de ce type a de bonnes chances de présenter des problèmes lors du redémarrage si la sauvegarde a été effectuée au niveau de fonctionnement standard (niveau 4 d'exécution standard). Dans notre exemple, le serveur de licence, s'il est lancé après une pseudo récupération de ce genre, se rend compte de l'incohérence des données du fichier et refuse d'exécuter le service attendu.

Sous Windows, tant que le système fonctionne et qu'il est opérationnel, de nombreux fichiers système ne peuvent pas être remplacés car le système les verrouille. Par exemple, les profils utilisateur en cours d'utilisation ne peuvent pas être restaurés. Le compte de connexion doit être changé ou le service correspondant arrêté.

Selon les éléments qui sont actifs sur le système au moment de l'exécution de la sauvegarde, il peut se produire une violation de la cohérence des données d'une application ayant pour conséquence des problèmes de redémarrage et d'exécution après la récupération.

La meilleure solution consisterait à effectuer la sauvegarde après avoir mis hors ligne les partitions correspondantes. Toutefois, dans la plupart des cas, cela n'est pas possible.

Présentation du processus

Pour déployer le processus de récupération après sinistre dans un environnement vaste comportant de nombreux systèmes, procédez comme suit :

1. **Planification**

   La planification doit être confiée au service d'administration informatique, qui devra :

   - Déterminer quels systèmes doivent être récupérés, ainsi que la fenêtre temporelle et le niveau de récupération nécessaires. Les systèmes critiques regroupent tous les systèmes permettant un fonctionnement correct du réseau (serveurs DNS, contrôleurs de domaine, passerelles, etc.), le Gestionnaire de cellule et les clients Agents de support.
   - Définir la méthode de récupération à utiliser (celle-ci aura un impact sur la préparation requise).
   - Définir une méthode pour obtenir les informations requises au moment de la récupération, tels que les supports contenant la base de données IDB et l'emplacement du fichier SRD mis à jour.
   - Elaborer une liste de vérification détaillée pour chaque étape, destinée à vous guider tout au long de la procédure.
   - Créer et exécuter un plan test destiné à vous assurer de la réussite de la récupération.

2. **Préparation à la récupération**

   Selon la méthode de récupération choisie, la préparation comprendra :

   Sur les systèmes UNIX :

   - La création d'outils tels que le disque auxiliaire avec le système d'exploitation minimal, les ressources réseau et l'Agent de disque Data Protector.
   - La création de scripts de pré-exécution destinés à collecter la structure du stockage et d'autres préparations spécifiques au client.

   Sur les systèmes Windows :

   - La mise à jour des **données de récupération système (SRD)** et leur stockage en lieu sûr (coffre). Pour des raisons de sécurité, vous devez restreindre l'accès aux fichiers SRD.

Sur tous les systèmes :

- L'exécution de tests à partir du plan de test de récupération après sinistre.
- La réalisation de sauvegardes correctes et cohérentes.

3. **Exécution des procédures de récupération**

   Conformez-vous aux procédures testées et aux listes de vérification établies pour récupérer le système endommagé.

Méthode de récupération après sinistre manuelle

Il s'agit d'une méthode de récupération après sinistre élémentaire et extrêmement souple : elle consiste à redonner au système cible la configuration du système d'origine. Pour obtenir des informations détaillées sur les systèmes d'exploitation pris en charge, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

Dans un premier temps, vous devez installer et configurer le DR OS. Ensuite, utilisez Data Protector pour restaurer les données (y compris les fichiers du système d'exploitation) en remplaçant les fichiers du système d'exploitation par ceux du système d'exploitation restauré.

Lors d'une récupération manuelle, il est important de regrouper les informations sur la structure de stockage, qui ne sont pas conservées dans des fichiers plats, telles que les informations de partition, les miroirs de disque et l'entrelacement.

Récupération après sinistre manuelle assistée d'un client Windows

Sur un client Windows, la procédure générale pour effectuer une récupération après sinistre manuelle assistée est la suivante :

Phase 1 :

1. Remplacez le matériel défectueux.
2. Réinstallez le système d'exploitation (créez et formatez les partitions requises).
3. Réinstallez les Service Packs.
4. Repartitionnez manuellement le disque et rétablissez la structure de stockage en réaffectant aux lecteurs leur lettre d'origine.

CONSEIL Vous pouvez combiner la phase 2 de la récupération après sinistre manuelle avec les outils de déploiement automatisé.

Phase 2 :

5. Exécutez la commande `drstart.exe` de Data Protector, qui installe le DR OS et lance la restauration des volumes critiques.
6. L'ordinateur doit être réinitialisé une fois que la commande `drstart` a terminé.
7. Si vous procédez à la récupération à partir d'un Gestionnaire de cellule ou si vous réalisez des tâches de récupération avancées, des étapes supplémentaires s'imposent. Pour plus d'informations, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.
8. Utilisez la procédure de restauration standard de Data Protector pour restaurer les données relatives aux utilisateurs et applications.

Phase 3 :

Récupération après sinistre d'un Gestionnaire de cellule UNIX

Sur un Gestionnaire de cellule UNIX, la procédure générale pour effectuer une récupération après sinistre manuelle est la suivante :

Phase 1 :

1. Remplacez le matériel défectueux.
2. Repartitionnez manuellement le disque et rétablissez la structure de stockage.
3. Réinstallez le système d'exploitation.
4. Réinstallez les correctifs.

Phase 2 :

5. Réinstallez le Gestionnaire de cellule Data Protector.
6. Pour simplifier la restauration de tous les autres fichiers depuis les supports, restaurez la dernière sauvegarde de la base de données IDB.
7. Pour rétablir la configuration antérieure, remplacez les informations de configuration de Data Protector (`/etc/opt/omni`) par les dernières informations de configuration Data Protector enregistrées dans la sauvegarde.

Phase 3 :

8. Utilisez la procédure de restauration standard de Data Protector pour restaurer les données relatives aux utilisateurs et applications.
9. Relancez le système.

Récupération après sinistre avec restitution de disque

Cette méthode est prise en charge sur les clients Windows et UNIX. Pour obtenir des informations détaillées sur les systèmes d'exploitation pris en charge, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

Sur les clients Windows, le disque du système endommagé (ou le disque de rechange pour le disque endommagé physiquement) est temporairement connecté à un système hôte. Une fois la restauration effectuée, le disque peut être reconnecté au système en panne et être amorcé. Sur les systèmes UNIX, le disque auxiliaire, disposant d'un système d'exploitation minimal avec gestion du réseau et sur lequel un Agent de disque Data Protector est installé, est utilisé pour réaliser la récupération après sinistre avec restitution de disque.

Il s'agit d'une méthode simple et rapide pour récupérer les clients. Sur les systèmes Windows, le système d'exploitation est également restauré automatiquement.

CONSEIL

Cette méthode est particulièrement utile avec les disques durs permutables à chaud car vous pouvez déconnecter un disque dur d'un système et en placer un nouveau tout en conservant l'alimentation électrique et le système opérationnels.

Récupération après sinistre avec restitution de disque pour un client Windows

La procédure de restitution de disque comprend les étapes générales suivantes sur un client Windows :

Phase 1 :

1. Connectez le disque de rechange à un système hôte.

2. Repartitionnez manuellement le disque de rechange et rétablissez la structure de stockage. Pour obtenir des informations sur les points de montage de Windows, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Phase 2 :

3. A l'aide de l'assistant Restitution de disque de Data Protector, restaurez les disques critiques du système original sur le disque de rechange.
4. Arrêtez le système d'hébergement, enlevez le disque de rechange et connectez-le au système cible. Vous n'avez pas besoin d'arrêter le système si vous utilisez un disque dur permutable à chaud.
5. Réamorcez le système cible à partir du disque de rechange.

Phase 3 :

6. Utilisez la procédure de restauration standard de Data Protector pour restaurer les données relatives aux utilisateurs et applications.

récupération après sinistre avec restitution de disque pour un client UNIX

Sur un client UNIX, la restitution de disque est effectuée à l'aide d'un disque auxiliaire (amovible) doté d'un système d'exploitation minimal avec la gestion du réseau et un agent Data Protector installés.

L'utilisation d'un disque auxiliaire sur un client UNIX comprend les étapes générales suivantes :

Phase 1 :

1. Remplacez le disque défectueux par un disque de rechange, connectez le disque auxiliaire au système cible et redémarrez le système avec le système d'exploitation minimal installé sur le disque auxiliaire.
2. Repartitionnez manuellement le disque de rechange, rétablissez la structure de stockage et configurez le disque de rechange pour le rendre amorçable.

Phase 2 :

3. En appliquant la procédure standard de restauration de Data Protector, restaurez le disque d'amorçage du système d'origine sur le disque de rechange (utilisez l'option `Restaurer dans`).
4. Arrêtez le système et retirez le disque auxiliaire. Vous n'avez pas besoin d'arrêter le système si vous utilisez un disque dur permutable à chaud.

5. Relancez le système.

Phase 3 :

6. Utilisez la procédure de restauration standard de Data Protector pour restaurer les données relatives aux utilisateurs et applications.

Récupération après sinistre automatique avancée (EADR)

Data Protector propose une procédure de récupération après sinistre avancée pour le Gestionnaire de cellule et les clients Windows. Pour obtenir des informations détaillées sur les systèmes d'exploitation pris en charge, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

La récupération après sinistre automatique avancée vous permet de regrouper automatiquement l'ensemble des données pertinentes relatives à l'environnement au moment de la sauvegarde. Pendant les sauvegardes complètes, les données requises pour l'installation et la configuration du DR OS temporaire sont "empaquetées" dans un gros **fichier image DR OS** unique et stockées sur la bande de sauvegarde (et éventuellement dans le Gestionnaire de cellule) pour chaque client sauvegardé de la cellule.

Outre ce fichier image, un **fichier de démarrage de la phase 1** (**fichier P1S**), requis pour le formatage et le partitionnement corrects du disque, est stocké sur le support de sauvegarde et dans le Gestionnaire de cellule. Lorsqu'un sinistre se produit, l'assistant de récupération après sinistre automatique avancée permet de restaurer l'image DR OS à partir du support de sauvegarde (si elle n'a pas été enregistrée dans le Gestionnaire de cellule pendant la sauvegarde complète) et de la convertir en une **image ISO pour CD de récupération après sinistre**. L'image ISO peut être gravée sur un CD à l'aide de n'importe quel graveur, puis utilisée pour amorcer le système cible.

Ensuite, Data Protector installe et configure automatiquement le DR OS, formate et partitionne les disques, et enfin rétablit le système d'origine à l'aide de Data Protector, tel qu'il était au moment de la sauvegarde.

IMPORTANT Il est recommandé de limiter l'accès aux supports de sauvegarde, images DR, fichiers SRD et CD de récupération après sinistre.

La procédure d'utilisation de la méthode de récupération après sinistre automatique avancée pour un client Windows comprend les étapes générales suivantes :

Procédure de récupération après sinistre automatique avancée

Phase 0 :

1. Réalisez une sauvegarde complète du client.
2. Utilisez l'assistant de récupération après sinistre automatique avancée pour préparer une image ISO pour CD de récupération après sinistre à partir du fichier image DR OS du système endommagé, et gravez cette image sur un CD. Si l'image DR OS n'a pas été enregistrée sur le Gestionnaire de cellule pendant la sauvegarde complète, l'assistant de récupération après sinistre automatique avancée la restaure à partir du support de sauvegarde.

IMPORTANT

Vous devez réaliser une nouvelle sauvegarde et préparer un nouveau CD de récupération après sinistre après chaque changement de matériel, logiciel ou configuration. Cela s'applique aussi aux modifications affectant le réseau, telles que les changements d'adresse IP ou de serveur DNS.

Phase 1 :

3. Remplacez le matériel défectueux.
4. Amorcez le système cible à partir du CD de récupération après sinistre et sélectionnez le champ d'application de la récupération. Cette récupération se déroule totalement sans surveillance.

Phase 2 :

5. Les volumes critiques (partition d'amorçage, système d'exploitation et partition contenant Data Protector) sont restaurés automatiquement.

Phase 3 :

6. Utilisez la procédure de restauration standard de Data Protector pour restaurer les données relatives aux utilisateurs et applications.

IMPORTANT Préparez un CD de rrécupération après sinistre à l'avance pour tous les systèmes critiques devant être restaurés en priorité (notamment pour tout serveur DNS, Gestionnaire de cellule, client Agent de support, serveur de fichiers, etc.).

One Button Disaster Recovery (OBDR)

La fonction One Button Disaster Recovery (OBDR) constitue une méthode de récupération Data Protector entièrement automatisée pour les clients Windows et le Gestionnaire de cellule, où l'intervention de l'utilisateur est réduite au minimum. Pour obtenir des informations détaillées sur les systèmes d'exploitation pris en charge, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

Cette procédure vous permet de regrouper automatiquement l'ensemble des données Windows pertinentes relatives à l'environnement au moment de la sauvegarde. Pendant une sauvegarde complète, les données requises pour l'installation et la configuration du DR OS temporaire sont "empaquetées" dans un fichier image OBDR unique, et stockées sur une bande de sauvegarde. Lorsqu'un sinistre survient, un périphérique OBDR (un périphérique de sauvegarde, capable d'émuler un CD-ROM) est utilisé pour amorcer le système cible directement à partir de la bande contenant le fichier image OBDR avec les informations de récupération après sinistre.

Ensuite, Data Protector installe et configure le DR OS, formate et partitionne les disques, et enfin rétablit le système d'exploitation d'origine à l'aide de Data Protector, tel qu'il était au moment de la sauvegarde.

IMPORTANT Vous devez préparer une nouvelle bande d'amorçage OBDR après chaque changement de matériel, logiciel ou configuration. Cela s'applique aussi aux modifications affectant la configuration du réseau, telles que les changements d'adresse IP ou de serveur DNS.

La procédure One Button Disaster Recovery pour un Gestionnaire de cellule comprend les étapes générales suivantes :

Procédure One Button Disaster Recovery

Phase 0 :

1. Vous devez disposer d'une sauvegarde OBDR (créez la spécification de sauvegarde à l'aide de l'assistant One Button Disaster Recovery de Data Protector).

Phase 1 :

2. Amorcez le système à partir de la bande de récupération et sélectionnez le champ d'application de la récupération.

Phase 2 :

3. Par défaut, les volumes critiques (partition d'amorçage, système d'exploitation et partition contenant Data Protector) sont restaurés.

Phase 3 :

4. Restaurez les partitions restantes éventuelles au moyen de la procédure de restauration standard de Data Protector.

IMPORTANT Il est recommandé de restreindre l'accès aux bandes d'amorçage OBDR.

Récupération automatique du système

La Récupération automatique du système (ASR) est un système automatisé sur les systèmes Windows, qui reconfigure un disque et rétablit son état initial (ou redimensionne les partitions si le nouveau disque est plus grand que le disque initial) dans le cas d'un sinistre. Le partitionnement de disque et la configuration de volume logique (formats de fichier, affectation de lettres de lecteur et caractéristiques de volume) en font partie. Grâce à la procédure ASR, la commande `drstart.exe` Data Protector peut ainsi installer le DR OS actif qui fournit à Data Protector l'accès aux disque, réseau, bande et système de fichiers.

Data Protector peut ensuite redonner au système cible la configuration du système d'origine et restaurer toutes les données utilisateur.

Pour obtenir des informations détaillées sur les systèmes d'exploitation pris en charge, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

La procédure de récupération automatique du système comprend les étapes générales suivantes sur un client Windows :

Procédure ASR

Phase 0 :

1. Réalisez une sauvegarde complète du client.
2. Préparez des disquettes ASR avec les données binaires de Data Protector et mettez à jour la première disquette après chaque changement de configuration.

Phase 1 :

3. Amorcez le système à partir du support d'installation de Windows et entrez dans le mode ASR en appuyant sur la touche **F2**.
4. Insérez la première disquette (à jour) du jeu de disquettes ASR.
5. Après le réamorçage, fournissez les informations relatives à l'emplacement de l'installation du système de récupération après sinistre et du fichier SRD (`a:\`).
6. Changez de disquettes lorsque vous y êtes invité.

Phase 2 :

7. Tous les objets critiques sont automatiquement restaurés. Réamorcez le système, puis retirez le support d'installation Windows et la disquette ASR.

Phase 3 :

8. Restauration des données relatives aux utilisateurs et applications au moyen de la procédure de restauration standard de Data Protector.

La procédure ASR permet de réaliser (une partie de) la préparation à un sinistre, ainsi que le repartitionnement et le reformatage de la partition d'amorçage. Data Protector fournit toutes les autres fonctionnalités, parmi lesquelles une administration centralisée simple, une sauvegarde hautes performances, une prise en charge haute disponibilité, des fonctions de restauration simples, mais aussi de contrôle, de génération de rapports et de notification, etc.

Présentation des méthodes de récupération après sinistre

Le tableau 2-6 à la page 124 offre une présentation des différentes méthodes de récupération après sinistre de Data Protector. Pour en savoir plus sur la matrice de la prise en charge des plates-formes, reportez-vous au tableau 2-7 à la page 128.

Tableau 2-6 Présentation des méthodes de récupération après sinistre

	Phase 0	**Phase 1**	**Phase 2**	**Phase 3**
Récupération après sinistre manuelle	Sauvegarde complète du client, sauvegarde de la base de données IDB (Gestionnaire de cellule uniquement). Mise à jour du fichier SRD (Windows uniquement). Collecte d'informations sur le système d'origine pour permettre l'installation et la configuration du DR OS.	Installation du DR OS avec prise en charge du réseau. Repartitionnement du disque et rétablissement de la structure de stockage initiale.	Exécution de la commande `drstart` pour restaurer automatiquement les volumes critiques. Etapes supplémentaires nécessaires pour réaliser les tâches de récupération avancées. Reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.	Restauration des données relatives aux utilisateurs et applications au moyen de la procédure de restauration standard de Data Protector.

Tableau 2-6 Présentation des méthodes de récupération après sinistre

	Phase 0	**Phase 1**	**Phase 2**	**Phase 3**
Récupération après sinistre avec restitution de disque (DDDR)	Sauvegarde complète du client, sauvegarde de la base de données IDB (Gestionnaire de cellule uniquement), création du disque auxiliaire (UNIX uniquement).	Windows : connexion d'un disque de rechange à un système hôte. UNIX : connexion du disque auxiliaire au système cible. Tous les systèmes : repartitionnement du disque de rechange et rétablissement de la structure de stockage initiale.	Windows : restauration des volumes critiques à l'aide de l'assistant DDDR, retrait du disque de rechange du système hôte et connexion de ce dernier au système cible. UNIX : restauration du disque d'amorçage du système d'origine sur le disque de rechange, retrait du disque d'amorçage auxiliaire. Tous les systèmes : redémarrage du système. Etapes supplémentaires nécessaires pour réaliser les tâches de récupération avancées. Reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.	Restauration des données relatives aux utilisateurs et applications au moyen de la procédure de restauration standard de Data Protector.

Tableau 2-6 Présentation des méthodes de récupération après sinistre

	Phase 0	**Phase 1**	**Phase 2**	**Phase 3**
Récupération après sinistre automatique avancée (EADR)	Sauvegarde complète du client, sauvegarde de la base de données IDB (Gestionnaire de cellule uniquement). Préparation et mise à jour du fichier SRD. Préparation du CD de récupération après sinistre.	Redémarrage du système à partir du CD de récupération après sinistre et sélection du champ d'application de la récupération.	Restauration automatique des volumes critiques. Etapes supplémentaires nécessaires pour réaliser les tâches de récupération avancées. Reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.	Restauration des données relatives aux utilisateurs et applications au moyen de la procédure de restauration standard de Data Protector.
One Button Disaster Recovery (OBDR)	Sauvegarde complète du client à l'aide de l'assistant OBDR. Préparation et mise à jour du fichier SRD.	Redémarrage du système cible à partir de la bande OBDR et sélection du champ d'application de la récupération.	Restauration automatique des volumes critiques.	Restauration des données relatives aux utilisateurs et applications au moyen de la procédure de restauration standard de Data Protector.

Tableau 2-6 Présentation des méthodes de récupération après sinistre

	Phase 0	**Phase 1**	**Phase 2**	**Phase 3**
Récupération automatique du système (ASR)	Sauvegarde complète du client, préparation de disquettes ASR avec le fichier SRD à jour et les données binaires de DP.	Amorçage du système à partir du support d'installation de Windows et passage en mode ASR. Insertion de la disquette ASR.	Les volumes critiques sont restaurés. Des étapes supplémentaires sont nécessaires pour réaliser les tâches de récupération avancées. Reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.	Restauration des données relatives aux utilisateurs et applications au moyen de la procédure de restauration standard de Data Protector.

Les étapes suivantes doivent être réalisées avant de pouvoir passer à la phase suivante :

- Phase 0 : une sauvegarde complète du client et une sauvegarde de la base de données IDB (Gestionnaire de cellule uniquement) doivent être effectuées, et une quantité suffisante d'informations doit être collectée par l'administrateur à partir du système d'origine pour permettre l'installation et la configuration du DR OS. Un disque d'amorçage auxiliaire doit être créé pour la récupération après sinistre avec restitution de disque sous UNIX.
- Phase 1 : le DR OS doit être installé et configuré et la structure de stockage d'origine doit être rétablie (tous les volumes sont prêts à être restaurés). Le disque de rechange pour la récupération après sinistre avec restitution de disque sous UNIX doit être rendu amorçable.
- Phase 2 : les volumes critiques sont restaurés. Des étapes supplémentaires sont nécessaires pour réaliser les tâches de récupération avancées. Reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.
- Phase 3 : vérifiez que les données d'application sont restaurées correctement (bases de données cohérentes, etc.).

Méthodes de récupération après sinistre et systèmes d'exploitation

Le tableau suivant peut être utilisé comme un index des combinaisons de méthodes de récupération après sinistre et de systèmes d'exploitation prises en charge. Les combinaisons sont décrites dans les sections suivantes.

REMARQUE Chaque méthode de récupération après sinistre fait l'objet de restrictions qu'il est important d'examiner avant sa mise en œuvre.

Tableau 2-7 Méthodes de récupération après sinistre prises en charge par système d'exploitation

	Gestionnaire de cellule	Client
Windows 2000	• Récupération après sinistre manuelle assistée • Récupération après sinistre automatique avancée • One Button Disaster Recovery	• Récupération après sinistre manuelle assistée • Récupération après sinistre avec restitution de disque • Récupération après sinistre automatique avancée • One Button Disaster Recovery

Tableau 2-7 Méthodes de récupération après sinistre prises en charge par système d'exploitation

	Gestionnaire de cellule	Client
Windows XP/Server 2003 32 bits[a]	• Récupération après sinistre manuelle assistée • Récupération automatique du système	• Récupération après sinistre manuelle assistée • Récupération après sinistre avec restitution de disque • Récupération automatique du système
Windows Server 2003 64 bits		• Récupération après sinistre manuelle assistée • Récupération automatique du système
HP UX 11.x	• Récupération après sinistre manuelle	• Récupération après sinistre manuelle • Récupération après sinistre avec restitution de disque
Solaris 7/8	• Récupération après sinistre manuelle	• Récupération après sinistre avec restitution de disque
Tru64/AIX		• Récupération après sinistre avec restitution de disque

a. La procédure ASR n'est pas disponible avec Windows XP Edition familiale et par conséquent, n'est pas prise en charge.

Autres méthodes de récupération après sinistre

Cette section compare le concept de récupération après sinistre de Data Protector avec les solutions proposées par d'autres fournisseurs. Plutôt que de nous lancer dans un débat approfondi, nous avons cherché à mettre en avant les aspects significatifs des autres méthodes de récupération existantes. Deux autres méthodes de récupération sont étudiées :

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

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

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

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

Récupération avec des outils tiers (pour Windows)

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

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

Il apparaît donc clairement que cette méthode implique l'utilisation de deux sauvegardes différentes avec des outils différents. Il s'agit généralement d'une tâche difficile à accomplir. Si vous mettez en œuvre

cette méthode dans une grande société, la surcharge administrative liée à la gestion des différentes versions des données (sauvegardes hebdomadaires) avec deux outils différents doit être prise en compte.

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

3 Gestion des supports et périphériques

Description du chapitre

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

Il s'organise comme suit :

Gestion des supports

Une fois le système de sauvegarde configuré, la gestion des supports devient l'une des tâches importantes à réaliser pour que la session continue de fonctionner sans interruption. La gestion de grandes opérations de sauvegarde implique souvent la gestion de plusieurs milliers de supports.

Fonctions de gestion des supports

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

- Supports regroupés en unités logiques appelées pools de supports : permet de travailler sur de grands groupes de supports; évite ainsi de gérer chacun des supports de façon individuelle.
- Data Protector assure le suivi de tous les supports et garde en mémoire : l'état de chacun d'eux, le délai d'expiration de la protection des données, la disponibilité des supports pour les sauvegardes, ainsi qu'un catalogue des sauvegardes effectuées sur chaque support.
- Stratégies de rotation automatisée des supports : évite de devoir gérer manuellement la rotation des bandes.
- Possibilité de définir explicitement les supports et les périphériques devant être utilisés pour la sauvegarde.
- Gestion des supports optimisée pour des types de périphériques déterminés, tels que les périphériques autonomes, de magasin et de bibliothèque, ainsi que les grands périphériques silo.
- Fonctionnement entièrement automatisé. Si le nombre de supports auxquels Data Protector peut accéder au niveau des périphériques de bibliothèque est suffisamment élevé, la fonctionnalité de gestion des supports permet d'exécuter des sauvegardes pendant des semaines sans intervention d'un opérateur pour s'occuper des supports.
- Reconnaissance et prise en charge des codes-barres assurées sur les périphériques silo et sur certaines grandes bibliothèques.
- Fonction de reconnaissance automatique des formats de support Data Protector et des autres formats de bandes courants.

- Data Protector ne permet d'écrire que sur des supports vierges qui ont été initialisés (formatés) dans Data Protector. Data Protector ne peut pas être utilisé pour écraser des formats de bandes externes lors d'une sauvegarde, cette restriction permettant d'éviter d'écraser par erreur des supports créés dans d'autres applications.
- Reconnaissance, suivi, affichage et gestion des supports utilisés par Data Protector et séparation de ces supports de ceux utilisés par d'autres applications au niveau des périphériques de bibliothèque et silo.
- Conservation dans un emplacement centralisé des informations sur les supports utilisés et partage de ces informations entre plusieurs cellules Data Protector.
- Prise en charge de la mise au coffre des supports.
- Création interactive ou automatisée de copies supplémentaires des données sur les supports.

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

Cycle de vie des supports

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

1. Préparation des supports pour la sauvegarde.

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

   Pour plus d'informations, reportez-vous à la section "Gestion des supports avant le début des sauvegardes" à la page 149.

2. Utilisation des supports pour la sauvegarde.

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

   Pour plus d'informations, reportez-vous à la section "Gestion des supports pendant une session de sauvegarde" à la page 151.

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

   Pour plus d'informations sur la mise au coffre, reportez-vous à la section "Gestion des supports après une session de sauvegarde" à la page 156.

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

5. Mise hors service des supports.

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

   Reportez-vous à la section "Détermination de l'état des supports" à la page 155.

Pools de supports

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

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

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

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

Plusieurs périphériques peuvent utiliser des supports du même pool.

Exemples de propriétés de pool de supports

Exemples de propriétés de pools :

- Ajout possible

  Permet à Data Protector d'ajouter des données aux supports de ce pool lors des sessions de sauvegarde ultérieures.

  Si cette option est désactivée, les supports contiendront uniquement des données d'une même session.

- Ajout possible aux incrémentales uniquement

  Une session de sauvegarde est ajoutée à un support uniquement en cas de sauvegarde incrémentale. Cette propriété permet de disposer d'un jeu complet de sauvegardes complètes et incrémentales sur le même support, dans la mesure où l'espace est suffisant.

- Stratégie d'allocation de supports

  Il existe plusieurs niveaux de rigueur concernant le choix des supports pour la sauvegarde. Ils s'échelonnent de strict (Data Protector requiert un support spécifique) à souple (Data Protector accepte tout support adéquat dans le pool, y compris les nouveaux supports).

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

Pour obtenir des informations sur les autres propriétés des pools de supports, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Pools de supports et répertoires `dcbf`

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

Pour obtenir des informations sur la partie DCBF de la base de données IDB et sur les répertoires `dcbf`, reportez-vous à la section “Architecture de la base de données IDB” à la page 206.

Utilisation des pools de supports

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

- Plate-forme système (un pool pour les systèmes UNIX, un autre pour les systèmes Windows 2000 et un autre pour les systèmes Windows XP).
- Par système (chaque système a son propre pool).
- Structure organisationnelle (tous les systèmes du service_A ont un pool et ceux du service_B un autre).
- Catégories de systèmes (grandes bases de données ou applications stratégiques).
- Type de sauvegarde (toutes les sauvegardes complètes utilisent un pool et toutes les sauvegardes incrémentales un autre).
- Combinaison des critères exposés ci-dessus, etc.

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

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

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

Pools de supports par défaut

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

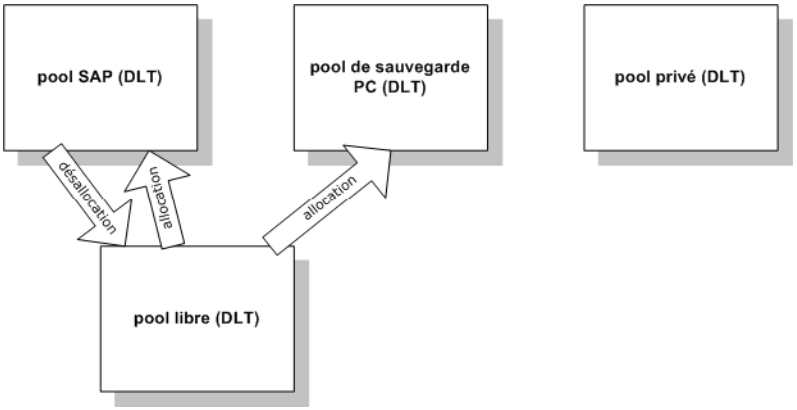
Pools libres

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

Qu'est-ce qu'un pool libre ?

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

Figure 3-1 **Pools libres**



Quand utilise-t-on un pool libre ?

Les supports sont déplacés entre les pools ordinaires et libres dans deux cas (figure 3-1) :

- L'allocation. Les supports sont déplacés d'un pool libre vers un pool ordinaire.
- La désallocation. Les supports sont déplacés d'un pool ordinaire vers un pool libre. Vous pouvez configurer le système pour que la désallocation s'exécute automatiquement. Par exemple, les supports du pool de sauvegarde PC illustré à la figure 3-1 ne sont pas automatiquement désalloués.

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

Certains pools classiques, par exemple le pool privé illustré à la figure 3-1, peuvent également être configurés pour ne pas partager de supports avec les pools libres.

Avantages d'un pool libre

Un pool libre présente les avantages suivants :

- Partage des supports libres entre les pools.

  Tous les supports libres (non protégés, vides) peuvent être regroupés dans un pool libre et partagés entre tous les pools de supports prenant en charge l'utilisation des pools libres.

- L'intervention de l'opérateur est limitée dans le cadre de la sauvegarde.

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

Propriétés d'un pool libre

Un pool libre :

- Est créé automatiquement lorsque vous configurez son utilisation. Vous ne pouvez pas supprimer les pools libres qui ont été utilisés ou qui ne sont pas vides.
- Est spécifique à un type de support, Data Protector ne prenant en charge qu'un pool libre par type de support (par exemple DDS).
- Est différent d'un pool ordinaire dans le sens où il ne propose pas d'options de stratégie d'allocation.
- Contient uniquement des supports Data Protector (supports inconnus ou vierges exclus).

Détermination de la qualité des supports

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

Limites des pools libres

Les limites des pools libres sont les suivantes :

- Vous ne pouvez pas créer de pool libre multiple pour le même type de support, car les pools libres sont créés automatiquement par Data Protector.
- Vous ne pouvez pas sélectionner différents facteurs d'état pour chaque pool. En revanche, tous les pools utilisant le pool libre utilisent les facteurs d'état configurés pour le pool libre.
- Un support protégé ne peut pas être déplacé vers un pool libre. De même, un support non protégé ne peut pas être déplacé vers un pool ordinaire si la désallocation automatique est activée sur ce pool.
- Vous ne pouvez pas utiliser d'opérations telles que l'importation, la copie, le recyclage sur des supports d'un pool libre.
- Les pools avec prise en charge de magasins ne peuvent pas utiliser de pool libre.

- Certaines incohérences provisoires peuvent apparaître dans les pools en cas d'utilisation de pools libres, par exemple lorsqu'un support non protégé situé dans un pool ordinaire attend le processus de désallocation.
- Si vous changez la protection des supports après son expiration (par exemple en Permanent), même si les supports se trouvent dans un pool libre, ils ne seront pas alloués pour la sauvegarde.

Pour obtenir des informations supplémentaires sur les pools libres, effectuez une recherche dans l'index de l'aide en ligne Data Protector à partir des mots clés "pools libres, caractéristiques".

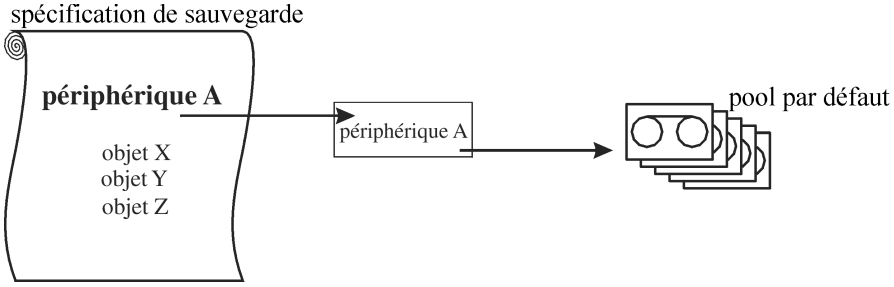
Exemples d'utilisation de pools de supports

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

Exemple 1

Dans le modèle proposé à la figure 3-2, tous les objets sont sauvegardés sur le même pool de supports. La spécification de sauvegarde ne fait référence à aucun pool, c'est la raison pour laquelle le pool par défaut, qui fait partie de la définition du périphérique, est utilisé.

Figure 3-2 Relation simple entre un périphérique et un pool de supports



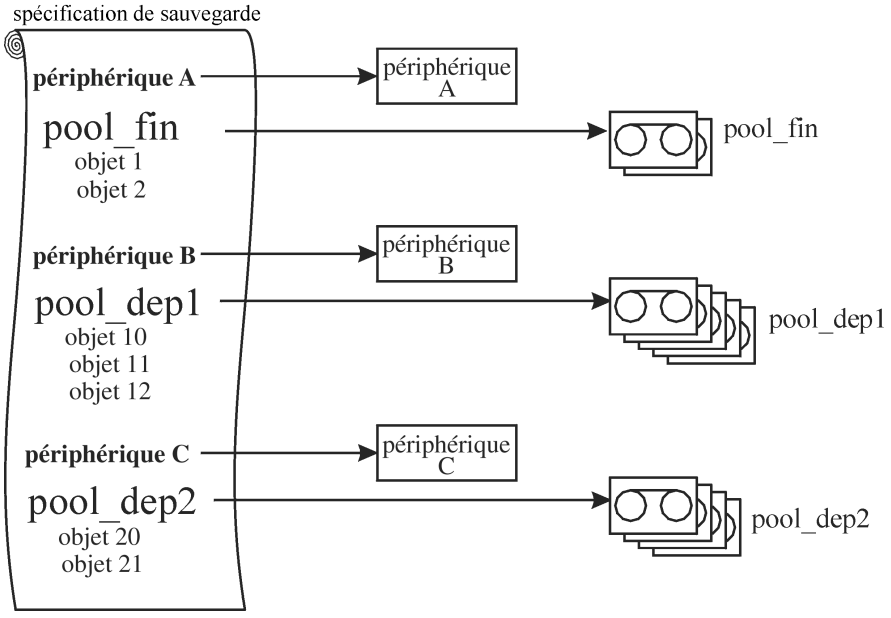
Exemple 2

Les grands périphériques de bibliothèque contiennent un certain nombre de lecteurs et de supports utilisés par différents services et applications. Vous pouvez configurer un pool de supports pour chaque service, comme le montre la figure 3-3, et choisir le lecteur dans la bibliothèque qui effectuera le transfert de données réel. La flèche qui relie une spécification de sauvegarde à un pool de supports indique que vous avez défini un pool de supports cible dans une spécification de sauvegarde.

Si vous ne précisez pas de pool de supports dans la spécification de sauvegarde, le pool par défaut, spécifié dans la définition du périphérique, est utilisé.

Pour obtenir plus d'informations sur la relation entre les pools de supports et les grands périphériques de bibliothèque, reportez-vous à la section "Grandes bibliothèques" à la page 170.

Figure 3-3 **Configuration des pools de supports pour les grandes bibliothèques**

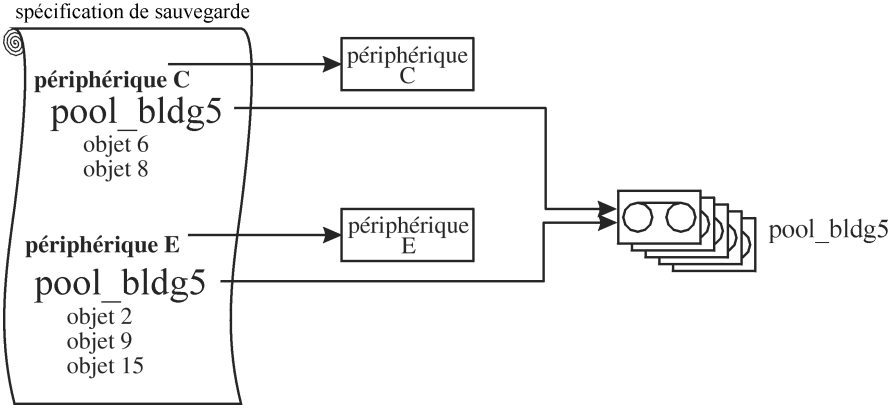


Exemple 3

Dans l'exemple présenté à la figure 3-4, plusieurs périphériques sont utilisés simultanément pour sauvegarder des données sur des supports d'un pool. Les performances sont améliorées grâce à l'utilisation de plusieurs périphériques en parallèle, quel que soit le pool utilisé.

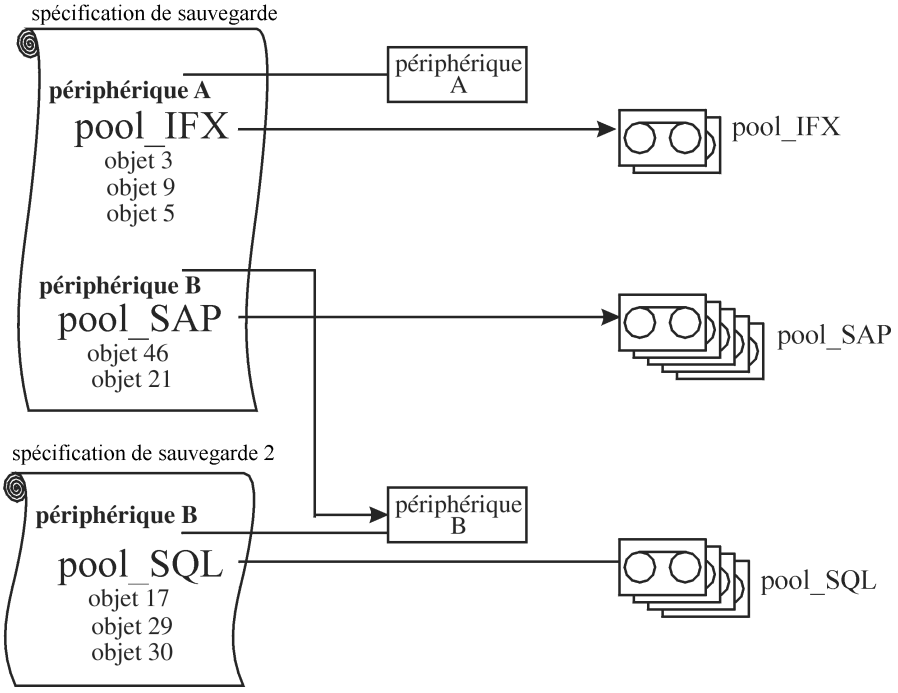
Pour plus d'informations, reportez-vous à la section "Listes de périphériques et partage de charge" à la page 161.

Figure 3-4 **Périphériques multiples, pool de supports unique**



Exemple 4 Plusieurs périphériques sont utilisés simultanément pour sauvegarder des données sur des supports de plusieurs pools. Si vous voulez utiliser le même périphérique avec différents pools, vous devez créer plusieurs spécifications de sauvegarde. Dans l'exemple ci-dessous, un pool de supports séparé est prévu pour chaque application de base de données.

Figure 3-5 **Périphériques multiples, pools de supports multiples**



Mise en œuvre d'une stratégie de rotation des supports

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

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

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

Les stratégies de sauvegarde traditionnelles utilisées avec les anciens outils de sauvegarde nécessitaient une stratégie de rotation des supports bien définie et planifiée, contrôlée par l'administrateur plutôt que par l'application de sauvegarde. Data Protector vous permet de mettre en œuvre une stratégie de rotation en spécifiant les options d'utilisation afin que la sélection des supports pour les sauvegardes ultérieures s'effectue automatiquement.

Rotation des supports et Data Protector

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

Rotation et gestion automatiques des supports

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

Supports requis pour la rotation

Estimation de la quantité de supports requis

La section suivante vous aidera à estimer la quantité de supports nécessaires pour une rotation complète :

- Déterminez si les supports disponibles peuvent être utilisés intégralement, ou bien si certains supports ont la propriété Sans possibilité d'ajout et ne peuvent être utilisés que partiellement.
- Déterminez quels systèmes seront sauvegardés, ainsi que l'espace requis sur les supports pour la sauvegarde des données associées. Vous pouvez par exemple utiliser le test de sauvegarde.
- Déterminez la fréquence de sauvegarde, par exemple le nombre de sauvegardes incrémentales à effectuer entre deux sauvegardes complètes.
- Déterminez le nombre de supports requis pour une génération de sauvegarde (une génération de sauvegarde étant constituée d'une sauvegarde complète et de toutes les sauvegardes incrémentales effectuées jusqu'à la sauvegarde complète suivante). Prenez également en compte la compression matérielle si vous avez prévu de l'utiliser avec les périphériques.
- Déterminez la durée pendant laquelle les supports seront protégés.
- Calculez le nombre de générations de sauvegarde qui pourront être créées avant que la première génération de sauvegarde ne soit écrasée.

A ce stade, vous devez être à même d'estimer la quantité de supports requis pour une rotation de supports complète. Il vous faudra peut-être prévoir des supports supplémentaires dans la mesure où :

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

Gestion des supports avant le début des sauvegardes

Vous devez initialiser ou formater les supports avant de pouvoir les utiliser pour la sauvegarde dans Data Protector. Vous pouvez les initialiser (formater) manuellement ou laisser Data Protector les initialiser (formater) automatiquement lorsqu'ils sont sélectionnés pour la sauvegarde. Reportez-vous à la section "Sélection des supports utilisés pour la sauvegarde" à la page 151.

Initialisation ou formatage des supports

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

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

Si les supports ne sont pas initialisés (formatés) avant la sauvegarde, Data Protector peut initialiser (formater) des supports vierges au cours de cette sauvegarde en utilisant des étiquettes par défaut, si la définition de la stratégie de pool le permet. La première sauvegarde sur ces supports prendra alors plus de temps. Pour plus d'informations, reportez-vous à la section "Sélection des supports utilisés pour la sauvegarde" à la page 151.

Etiquetage des supports Data Protector

Comment les supports sont-ils étiquetés dans Data Protector ?

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

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

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

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

Comment sont utilisées les étiquettes ?

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

Champ Emplacement

Les supports de sauvegarde sont généralement stockés à différents emplacements. Par exemple, les sauvegardes doivent être stockées sur site pour que les données puissent être rapidement restaurées, tandis que les supports contenant une copie des données sauvegardées sont généralement stockés hors site pour des raisons de sécurité.

Un champ d'emplacement est disponible dans Data Protector pour chaque support. L'opérateur peut utiliser ce champ à sa convenance. Le champ Emplacement permet de localiser les supports. Exemples de définitions d'emplacement pertinentes : bibliothèque, hors site, coffre_1, etc.

Le paramètre d'emplacement des supports est également utile si la version d'objet que vous souhaitez restaurer existe sur plusieurs jeux de supports. Vous pouvez définir la priorité d'emplacement des supports qui influencera la sélection du jeu de supports utilisé pour la restauration. Pour plus d'informations sur la sélection des supports utilisés pour la restauration, reportez-vous à la section “Sélection du jeu de supports” à la page 107.

Gestion des supports pendant une session de sauvegarde

Que se passe-t-il pendant la sauvegarde ?

Pendant une session de sauvegarde, Data Protector sélectionne automatiquement les supports et effectue un suivi des données sauvegardées et des supports utilisés. Cela simplifie la gestion des supports, car l'opérateur n'a pas besoin de savoir exactement quelles données ont été sauvegardées, ni quels supports ont été utilisés. Les objets sauvegarde ayant été sauvegardés lors d'une même session constituent un jeu de supports.

Cette section traite des sujets suivants :

- Comment Data Protector sélectionne-t-il les supports qui seront utilisés pour la sauvegarde ?
- Comment les sauvegardes complètes et incrémentales sont-elles ajoutées aux supports ?
- Comment l'état des supports est-il défini ?

Pour obtenir plus d'informations, reportez-vous aux sections suivantes :

- "Sauvegardes complètes et incrémentales" à la page 68
- "Pools de supports" à la page 138

Sélection des supports utilisés pour la sauvegarde

Data Protector sélectionne automatiquement les supports en fonction des stratégies d'allocation des supports. Cela simplifie considérablement la gestion et le traitement des supports étant donné que l'opérateur de sauvegarde n'a pas besoin d'administrer manuellement les supports pour la sauvegarde.

Stratégie d'allocation de supports

Les stratégies d'allocation des supports permettent d'influer sur le mode de sélection des supports. Vous pouvez choisir une stratégie souple, selon laquelle tout support approprié est utilisé pour la sauvegarde, y compris les nouveaux supports et les supports vierges ou une stratégie stricte, selon laquelle les supports doivent être disponibles dans un ordre prédéfini pour faciliter une utilisation équilibrée des supports. Vous pouvez en outre utiliser une liste de préallocation.

Préallocation de supports

Data Protector vous permet de spécifier explicitement les supports d'un pool à utiliser pour une sauvegarde. Pour ce faire, vous devez avoir recours à une liste de préallocation et combiner celle-ci à une stratégie d'allocation stricte. Les supports sont alors utilisés dans l'ordre spécifié. Si les supports n'apparaissent pas dans cet ordre, Data Protector émet une demande de montage.

Etat des supports

L'état des supports influe également sur la sélection des supports utilisés pour la sauvegarde. Par exemple, les supports en bon état sont utilisés en priorité par rapport aux supports d'état passable. Pour plus d'informations, reportez-vous à la section "Détermination de l'état des supports" à la page 155.

Ajout de données aux supports pendant une session de sauvegarde

Pour optimiser au maximum l'utilisation de l'espace disponible sur les supports et l'efficacité de la sauvegarde et de la restauration, vous pouvez définir la façon dont l'espace laissé sur le support par la sauvegarde précédente sera traité par Data Protector. Pour ce faire, vous devez définir une stratégie d'utilisation de supports.

Stratégie d'utilisation de supports

Les stratégies d'utilisation de supports disponibles sont énoncées ci-dessous :

Ajout possible Lors d'une session de sauvegarde, le système commence par écrire les données au niveau de l'espace restant sur le dernier support utilisé lors de la session de sauvegarde précédente. L'écriture des données sur les autres supports requis dans le cadre de cette session commence au début de la bande : seules des bandes non protégées ou de nouvelles bandes peuvent donc être utilisées. L'ajout de supports permet d'économiser de l'espace sur les supports mais peut aussi compliquer la mise au coffre car un support peut contenir des données provenant de différents jeux de supports.

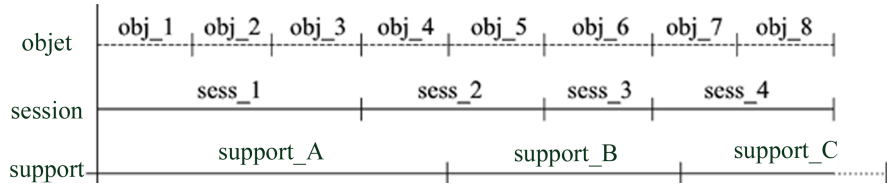
Sans possibilité d'ajout Lors d'une session de sauvegarde, le système commence par écrire les données au début du premier support disponible pour la sauvegarde. Un support ne peut pas contenir de données issues de deux sessions différentes. Cette stratégie simplifie la mise au coffre.

Ajout possible aux incrémentales uniquement Une session de sauvegarde est ajoutée à un support uniquement en cas de sauvegarde incrémentale. Cette propriété permet de disposer d'un jeu complet de sauvegardes complètes et incrémentales sur le même support, dans la mesure où l'espace est suffisant.

Distribution d'objets sur des supports

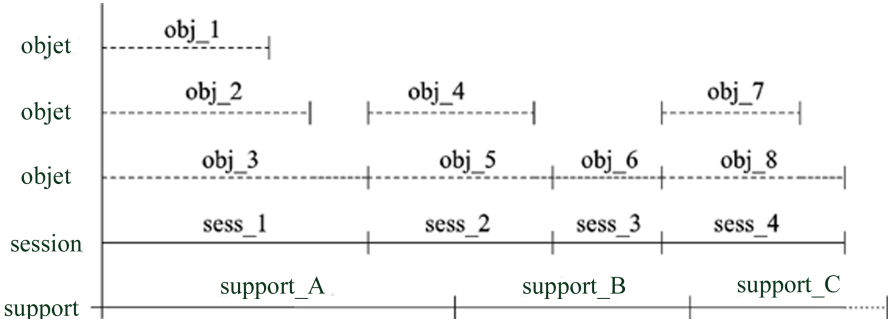
Les figures suivantes présentent quelques exemples de distribution d'objets sur des supports :

Figure 3-6 Sessions et objets multiples par support, écritures séquentielles



La figure 3-6 présente un exemple de huit écritures séquentielles sur quatre sessions, utilisant la stratégie d'utilisation de supports avec ajout possible. Les données ont été écrites en quatre sessions, objet par objet. Les trois supports appartiennent au même pool de supports. Le *support_A* et le *support_B* sont déjà saturés, alors que le *support_C* dispose encore d'espace.

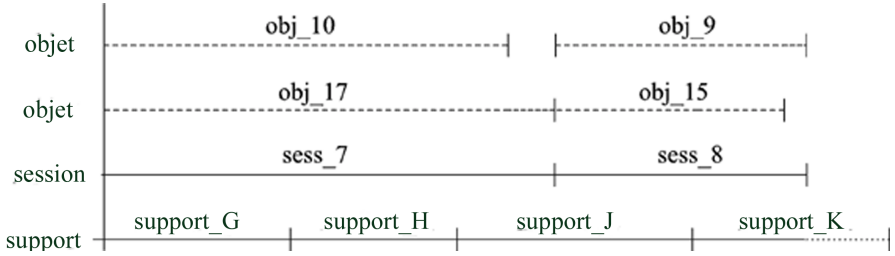
Figure 3-7 Sessions et objets multiples par support, écritures simultanées



La figure 3-7 présente un exemple de huit objets écrits sur quatre sessions, les paramètres de simultanéité permettant des écritures simultanées. Dans ce cas, *obj_1, obj_2* et *obj_3* ont été sauvegardés

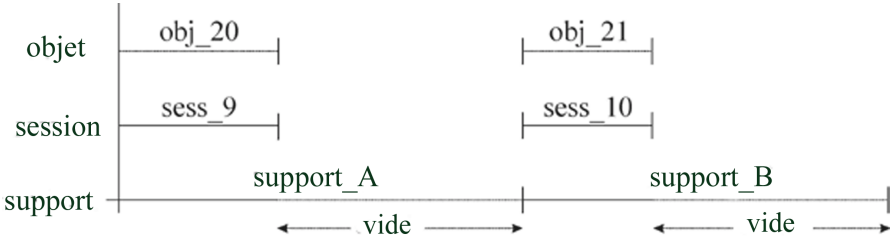
simultanément lors de *sess_1* ; *obj_4* et *obj_5* ont été sauvegardés simultanément lors de *sess_2*, etc. *Obj_1* peut provenir de *system_A* et *obj_2* de *system_B*, ou ils peuvent provenir tous deux de différents disques sur le même système. Les ajouts sont possibles dans le cadre de cette stratégie d'utilisation des supports.

Figure 3-8 **Supports multiples par session, supports multiples par objet**



La figure 3-8 présente un exemple de quatre objets sauvegarde ayant été sauvegardés lors de deux sessions, les objets de la première paire ayant été écrits simultanément au cours de *sess_7* et ceux de la seconde au cours de *sess_8*. Notez qu'un objet peut s'étendre sur plusieurs supports. Les ajouts sont possibles dans le cadre de cette stratégie d'utilisation des supports.

Figure 3-9 **Chaque objet est inscrit sur un support séparé**



Dans l'exemple présenté à la figure 3-9, une spécification de sauvegarde est utilisée par objet et la stratégie d'utilisation de supports appliquée est celle sans ajout possible. Le nombre de supports utilisé est supérieur. Si l'on combine cette méthode à la stratégie Ajout possible aux incrémentales uniquement, les sauvegardes incrémentales de l'objet sont écrites sur le même support.

Pour obtenir plus d'informations sur les répercussions des stratégies de sauvegardes complètes et incrémentales sur les performances de la restauration et de l'utilisation des supports, reportez-vous à la section "Sauvegardes complètes et incrémentales" à la page 68.

Ecriture de données sur plusieurs jeux de supports pendant la sauvegarde

Pendant une session de sauvegarde, vous pouvez écrire simultanément tout ou partie des objets sur plusieurs jeux de supports, à l'aide de la fonction de mise en miroir d'objet de Data Protector. Pour plus d'informations, reportez-vous à la section "Mise en miroir d'objet" à la page 101.

Détermination de l'état des supports

Facteurs d'état des supports

Data Protector détermine l'état des supports utilisés à l'aide de **facteurs d'état des supports**. L'état du support le plus médiocre dans un pool détermine l'état de l'ensemble du pool. Par exemple, dès que l'état d'un support dans un pool est médiocre, l'état du pool devient médiocre. Lorsque ce support particulier est supprimé du pool, l'état redevient soit passable, soit bon.

Les supports peuvent présenter trois états : bon, passable ou médiocre.

L'état est défini en fonction des éléments suivants, support par support :

- Nombre d'écrasements

  Le degré de vétusté d'un support est déterminé par le nombre d'écrasements réalisés depuis le début de son cycle de vie. Le support se voit attribuer l'état "médiocre" dès qu'il dépasse le nombre limite d'écrasements.

- Age des supports

  L'âge d'un support est calculé en fonction du nombre de mois écoulés depuis son formatage ou initialisation. Le support se voit attribuer l'état "médiocre" dès qu'il dépasse le nombre limite de mois.

- Erreurs de périphérique

  Un support peut se voir attribuer l'état "médiocre" suite à certaines erreurs de périphérique. Si une erreur se produit au niveau du périphérique pendant une sauvegarde, le support utilisé pour la sauvegarde dans ce périphérique se voit attribuer l'état "médiocre".

Gestion des supports après une session de sauvegarde

Une fois les données écrites sur les supports, vous devez prendre les mesures nécessaires pour protéger les supports et les données qu'ils contiennent. Prenez en compte les points suivants :

- Protection des supports contre les écrasements.

  Cette protection a été définie au moment de la configuration de la sauvegarde, mais vous pouvez la modifier après la sauvegarde. Pour plus d'informations sur la protection des données et du catalogue, reportez-vous à la section "Conservation des données sauvegardées et des informations sur les données" à la page 75.

- Protection des supports contre les dommages physiques.

  Les supports contenant des données permanentes peuvent être stockés dans un endroit sûr.

- Copie des données sauvegardées et conservation des copies dans un endroit sûr

  Reportez-vous à la section "Duplication de données sauvegardées" à la page 93.

Les sections suivantes décrivent la manière dont les supports sont mis au coffre et la restauration à partir des supports en question.

Mise au coffre

Qu'est-ce que la mise au coffre ?

La mise au coffre est une procédure consistant à stocker en lieu sûr des supports contenant des données importantes ; les supports sont ainsi stockés pendant une période déterminée. Le lieu où sont stockés les supports est généralement appelé **coffre**.

Les fonctions suivantes permettent la mise au coffre dans Data Protector :

- Stratégies de protection des données et du catalogue.
- Sélection et éjection des supports d'une bibliothèque.

- Le champ `emplacement de supports` indique l'emplacement physique des supports.
- Rapport indiquant les supports utilisés pour la sauvegarde au cours d'une période donnée.
- Rapport indiquant les spécifications de sauvegarde ayant utilisé des supports spécifiques lors de la sauvegarde.
- Rapport sur les supports stockés à un emplacement spécifique avec une protection de données expirant à un moment particulier.
- Présentation de la liste des supports nécessaires à la restauration de données spécifiques et des emplacements physiques où sont stockés ces supports.
- Filtrage des supports affichés selon des critères spécifiques.

Implémentation de la mise au coffre

L'implémentation de la mise au coffre dépend de la stratégie de sauvegarde adoptée par l'entreprise et de sa politique de gestion des données et des supports. Elle comporte généralement les étapes suivantes :

1. Spécification des stratégies de protection de données et du catalogue lors de la configuration des spécifications de sauvegarde.
2. Configuration d'un coffre dans Data Protector. Cela consiste principalement à spécifier le nom du coffre que vous utiliserez pour les supports, par exemple : Coffre_1.
3. Mise en place de la stratégie de gestion des supports appropriée pour les supports du coffre.
4. En option, création de copies supplémentaires des données sauvegardées à des fins de mise au coffre, utilisation de la fonctionnalité de mise en miroir d'objet pendant la sauvegarde ou de la fonctionnalité de copie d'objet ou de copie de supports après la sauvegarde.
5. Sélection des supports à mettre au coffre, éjection des supports et stockage dans le coffre.
6. Sélection des supports du coffre contenant des données expirées et insertion de ces supports dans une bibliothèque.

Exemple de mise au coffre

Supposons que la stratégie de sauvegarde de votre entreprise exige que les données soient sauvegardées de façon quotidienne. Chaque semaine, une sauvegarde complète doit être stockée dans un coffre où elle doit

rester disponible pendant les cinq années qui suivent. Vous devez être en mesure de restaurer facilement les données de toutes les sauvegardes des années précédentes, stockées dans le coffre. Au bout des cinq années, les supports du coffre peuvent être réutilisés.

Les paramètres suivants de Data Protector doivent être sélectionnés : sauvegarde complète une fois par semaine et sauvegardes incrémentales quotidiennes, protection des données réglée sur cinq ans et protection de catalogue réglée sur un an. Vous pourrez donc simplement explorer et restaurer des données pendant un an et les données resteront disponibles pendant cinq ans pour restauration à partir des supports. Les supports créés lors de la sauvegarde complète sont copiés et stockés dans un coffre. Au bout d'un an, Data Protector supprime automatiquement les informations détaillées de la base de données IDB relatives aux données contenues sur les supports, libérant ainsi de l'espace dans la base de données pour de nouvelles informations.

Restauration à partir de supports stockés dans un coffre

La restauration des supports stockés dans un coffre est identique à celle réalisée à partir de tout autre support. Selon les stratégies de protection des données et du catalogue que vous aurez choisies, vous devrez éventuellement effectuer quelques étapes supplémentaires :

1. Récupérer les supports stockés dans le coffre et les insérer dans un périphérique.
2. Si la protection de catalogue est toujours valide dans le cas de ces supports, vous pouvez restaurer les données souhaitées en les sélectionnant simplement à l'aide de l'interface utilisateur Data Protector.

   Si la protection de catalogue pour les supports est arrivée à expiration, Data Protector ne dispose pas d'informations détaillées sur les données sauvegardées. Vous devez effectuer la restauration en spécifiant manuellement quels fichiers ou répertoires vous souhaitez restaurer. Vous pouvez également restaurer l'objet entier sur un disque de rechange, puis rechercher des fichiers et répertoires dans le système de fichiers restauré.

CONSEIL Pour obtenir de nouveau les informations détaillées sur les fichiers et répertoires sauvegardés sur les supports après expiration de la protection de catalogue, exportez ces supports puis réimportez-les. Précisez ensuite que vous souhaitez lire les données du catalogue des détails de ces supports. Vous serez de nouveau en mesure de sélectionner des fichiers et des répertoires dans l'interface utilisateur Data Protector.

Pour plus d'informations sur la manière dont les stratégies de protection de données et du catalogue influent sur les restaurations, reportez-vous à la section "Conservation des données sauvegardées et des informations sur les données" à la page 75.

Périphériques

Data Protector prend en charge un certain nombre de périphériques disponibles sur le marché. Reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector* pour obtenir une liste récente des périphériques pris en charge.

Utilisation des périphériques dans Data Protector

Pour pouvoir utiliser un périphérique dans Data Protector, vous devez le configurer dans la cellule Data Protector. Lorsque vous configurez un périphérique, vous devez lui attribuer un nom, lui associer un pool de supports et définir des options spécifiques, telles que la prise en charge des codes-barres ou des bandes nettoyantes. La procédure de configuration de périphériques est simplifiée par l'assistant qui vous guide tout au long des étapes et qui peut détecter et configurer automatiquement des périphériques. Le même périphérique physique peut être défini plusieurs fois avec différentes propriétés d'utilisation dans Data Protector, par exemple, sans compression de données matérielles dans un cas et avec compression de données matérielles dans un autre. Pour ce faire, vous devez spécifier des noms de périphérique (logique) différents.

Les sections suivantes décrivent certaines fonctionnalités liées spécifiquement aux périphériques et expliquent le mode de fonctionnement de Data Protector associé à différents périphériques.

Prise en charge de la console de gestion de bibliothèque

De nombreuses bibliothèques de bandes modernes disposent d'une console d'administration qui permet de configurer, de gérer ou de contrôler les bibliothèques à partir d'un système distant. La portée des tâches pouvant être effectuées à distance dépend de l'implémentation de la console d'administration.

Data Protector simplifie l'accès à l'interface de la console d'administration de bibliothèque. Il est possible de spécifier l'URL (adresse Internet) de la console d'administration pendant le processus de configuration ou de reconfiguration de la bibliothèque. En sélectionnant un élément de menu dédié dans l'interface utilisateur, on appelle un navigateur Web et l'interface de la console est automatiquement chargée.

Pour obtenir une liste des types de périphériques sur lesquels cette fonction est disponible, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

IMPORTANT

Avant d'utiliser la console d'administration de la bibliothèque, sachez que certaines opérations effectuées au moyen de la console peuvent interférer avec vos tâches d'administration de supports et/ou vos sessions de sauvegarde et de restauration.

TapeAlert

TapeAlert est un utilitaire de messagerie et de surveillance d'état des périphériques à bandes qui facilite la détection des problèmes pouvant avoir un impact sur la qualité de la sauvegarde. TapeAlert envoie des alarmes ou des messages d'erreur faciles à interpréter au moment où les problèmes surgissent (utilisation de bandes usées, défauts matériels d'un périphérique, etc.), et propose des solutions pour y remédier.

Data Protector prend intégralement en charge TapeAlert 2.0, tant que les périphériques connectés proposent également cette fonctionnalité.

Listes de périphériques et partage de charge

Périphériques multiples pour la sauvegarde

Lorsque vous configurez une spécification de sauvegarde, vous pouvez spécifier plusieurs périphériques autonomes ou plusieurs lecteurs dans un périphérique de bibliothèque qui seront utilisés pour cette opération. Cela permet d'accélérer l'opération, les données étant sauvegardées en parallèle sur plusieurs périphériques (lecteurs).

Equilibrage de l'utilisation des périphériques

Par défaut, Data Protector équilibre automatiquement la charge (l'utilisation) des périphériques afin de les utiliser de manière uniforme. C'est ce qu'on appelle **partage de charge**. Ce procédé permet d'optimiser l'utilisation des périphériques en équilibrant le nombre des objets sauvegardés sur chacun. Cette opération s'effectuant automatiquement pendant la sauvegarde, l'utilisateur n'a pas besoin de gérer l'affectation des objets aux périphériques utilisés au cours de la session ; il lui suffit de spécifier les périphériques à utiliser.

Quand utiliser le partage de charge ?

Utilisez le partage de charge lorsque :

- Vous sauvegardez un grand nombre d'objets.
- Vous utilisez des périphériques de bibliothèque (changeur automatique) avec plusieurs lecteurs.

- Vous n'avez pas besoin de savoir sur quels supports seront sauvegardés les objets.
- Vous disposez d'une bonne connexion réseau.
- Vous souhaitez augmenter la fiabilité des sauvegardes. En cas d'échec d'un périphérique, Data Protector redirige automatiquement la sauvegarde vers d'autres périphériques sélectionnés à partir d'une liste de périphériques.

Quand ne pas utiliser le partage de charge ?

N'utilisez pas le partage de charge lorsque :

- Vous voulez sauvegarder un petit nombre d'objets volumineux. Dans ce cas, Data Protector ne peut généralement pas équilibrer la charge entre les périphériques de façon efficace.
- Vous voulez sélectionner les périphériques sur lesquels seront sauvegardés les objets.

Chaînage de périphériques

Data Protector vous permet de définir plusieurs périphériques autonomes en tant que chaîne de périphériques. Lorsqu'un support est plein dans un périphérique, la sauvegarde se poursuit automatiquement sur le support du périphérique suivant dans la chaîne de périphériques.

Périphérique en mode continu et simultanéité

Qu'est-ce qu'un périphérique en mode continu ?

Pour optimiser les performances d'un périphérique, celui-ci doit être alimenté en continu. On dit qu'un périphérique fonctionne en mode continu s'il peut fournir un volume de données suffisant au support pour que celui-ci avance en continu. Dans le cas contraire, la bande du support doit être arrêtée pendant que le périphérique attend les données supplémentaires. En d'autres termes, si la vitesse à laquelle les données sont écrites sur la bande est inférieure ou égale à celle à laquelle le système informatique les fournit au périphérique, ce dernier fonctionne en mode continu. Dans des infrastructures de sauvegarde en réseau, cela mérite une attention particulière. Dans le cadre d'une sauvegarde locale, les disques et les périphériques étant reliés au même système, une simultanéité de 1 peut suffire si vos disques sont suffisamment rapides.

Comment configurer un périphérique en mode continu ?

Pour permettre au périphérique de fonctionner en mode continu, une quantité de données suffisante doit lui être envoyée. Pour parvenir à cet objectif, Data Protector démarre plusieurs Agents de disque pour chaque Agent de support écrivant des données sur le périphérique.

Simultanéité des Agents de disque

La **simultanéité de sauvegarde des Agents de disque** correspond au nombre d'Agents de disque lancés pour chaque Agent de support ; ce nombre peut être modifié par le biais des options avancées liées au périphérique ou lors de la configuration d'une sauvegarde. Data Protector fournit des valeurs par défaut qui conviennent dans la plupart des cas. Par exemple, pour un périphérique DDS standard, deux Agents de disque envoient suffisamment de données pour que le périphérique fonctionne en mode continu. Si vous utilisez un périphérique de bibliothèque équipé de plusieurs lecteurs et que chaque lecteur est contrôlé par un Agent de support, vous pouvez régler la simultanéité séparément pour chaque lecteur.

Performances accrues

Lorsqu'elle est correctement configurée, la simultanéité de sauvegarde améliore les performances de la sauvegarde. Par exemple, si un périphérique de bibliothèque dispose de quatre lecteurs, chacun étant contrôlé par un Agent de support et chaque Agent de support recevant des données de deux Agents de disque simultanément, les données de huit disques sont sauvegardées simultanément.

Le fonctionnement en mode continu d'un périphérique dépend également d'autres facteurs, tels que la charge du réseau et la taille de bloc des données écrites sur le périphérique.

Pour obtenir d'autres informations à ce sujet, reportez-vous à la section "Sessions de sauvegarde" à la page 256.

Flux de données multiples

Data Protector permet de sauvegarder simultanément différentes parties d'un disque via plusieurs périphériques. Cette fonction permet de sauvegarder des disques rapides et de grande capacité sur des périphériques relativement lents. Plusieurs Agents de disque lisent les données du disque en parallèle et les envoient à plusieurs Agents de support. Cette méthode accélère la procédure de sauvegarde, à condition de prendre en compte les éléments suivants :

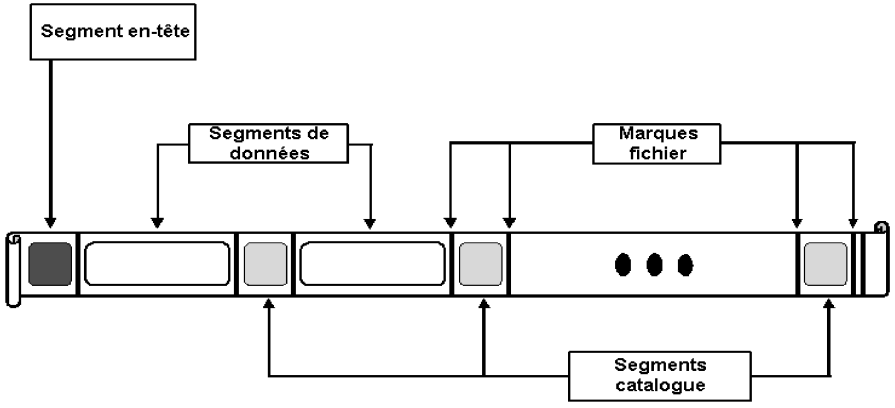
Si un point de montage a été sauvegardé via plusieurs Agents de disque, les données sont contenues dans plusieurs objets. Pour restaurer la totalité du point de montage, vous devez définir toutes les parties de celui-ci dans une spécification de sauvegarde unique, puis restaurer l'ensemble de la session.

Taille de segment

Un support est composé de segments de données, de segments de catalogue et d'un segment d'en-tête. Les informations d'en-tête sont stockées dans le segment d'en-tête, dont la taille est identique à celle du bloc. Les données sont enregistrées dans des blocs de données des segments de données. Les informations concernant chaque segment de données sont stockées dans les blocs de catalogue du segment de catalogue correspondant. Ces informations sont tout d'abord stockées dans la mémoire de l'Agent de support, puis écrites dans un segment de catalogue sur le support, ainsi que dans la base de données IDB. Tous les segments sont séparés par des marques comme le montre la figure 3-10.

REMARQUE Certaines technologies de bande limitent le nombre de marques de fichier par support. Assurez-vous que la taille de votre segment n'est pas trop réduite.

Figure 3-10 Format de données



La taille de segment, mesurée en méga-octets, correspond à la taille maximale des segments de données. Si vous sauvegardez un grand nombre de petits fichiers, la taille de segment réelle peut être limitée par la taille maximale des segments de catalogue. La taille de segment peut

être configurée par l'utilisateur pour chaque périphérique. Elle influe sur la rapidité d'une restauration. Une taille de segment réduite limite l'espace disponible sur le support pour les données : en effet, chaque segment dispose d'une marque qui utilise de l'espace sur les supports. Cependant, un grand nombre de marques de fichier permettent d'accélérer les restaurations, un Agent de support pouvant localiser plus rapidement le segment contenant les données à restaurer. La taille de segment optimale dépend du type de support utilisé dans le périphérique et du type de données à sauvegarder. Par exemple, la taille de segment par défaut du support DLT est de 150 Mo.

Taille de bloc

Les données contenues dans les segments sont en fait stockées dans des blocs et les informations de catalogue sont écrites dans des blocs de catalogue. Le périphérique traite les données par unités selon une taille de bloc spécifique du type de périphérique. Data Protector permet de régler la taille des blocs envoyés au périphérique. La taille de bloc par défaut pour l'ensemble des périphériques est de 64 Ko.

Vous pouvez améliorer les performances en augmentant la taille de bloc. Vous devez effectuer le changement de taille de bloc *avant* le formatage des bandes. Par exemple, une bande écrite avec la taille de bloc par défaut ne peut pas être complétée avec une taille de bloc différente.

REMARQUE Utilisez la même taille de bloc pour tous les supports dans un pool en mode Ajout possible. Data Protector ne peut ajouter des données à un support que si les tailles de bloc concordent.

Nombre de mémoires tampon utilisées par les Agents de disque

Les Agents de disque et les Agents de support Data Protector utilisent des mémoires tampon pour stocker les données à transférer. La mémoire est divisée en plusieurs zones tampon (une pour chaque Agent de disque, en fonction du nombre de périphériques fonctionnant simultanément). Chaque zone tampon est composée de 8 mémoires tampon d'Agent de disque (de la même taille que celle du bloc configuré pour le périphérique).

Vous pouvez remplacer cette valeur par tout nombre compris entre 1 et 32, bien que cela soit rarement nécessaire. Ces paramètres peuvent être changés pour deux raisons principales :

- Mémoire insuffisante

  La mémoire partagée requise par un Agent de support peut être calculée de la manière suivante :

  ```
  Simultanéité_AD*Nbre_mémoires_tampon*Taille_de_bloc
  ```

  En réduisant le nombre de mémoires tampon de 8 à 4, par exemple, vous diminuez de 50 % la quantité de mémoire utilisée et améliorez ainsi les performances.

- Mode continu

  Si la bande passante du réseau varie sensiblement au cours de la sauvegarde, il est important que l'Agent de support possède suffisamment de données prêtes à être écrites pour alimenter le périphérique en mode continu. Dans ce cas, augmentez le nombre de mémoires tampon.

Verrouillage de périphérique et noms de verrouillage

Noms de périphérique

Lorsque vous configurez des périphériques à l'aide de Data Protector, vous pouvez définir le même périphérique physique plusieurs fois avec des caractéristiques différentes. Pour ce faire, il suffit d'attribuer des noms différents à un même périphérique dans Data Protector. Par exemple, bien que cela ne soit pas recommandé, un périphérique autonome DDS peut être configuré comme périphérique compressé, puis comme périphérique non compressé.

Conflit de périphériques physiques

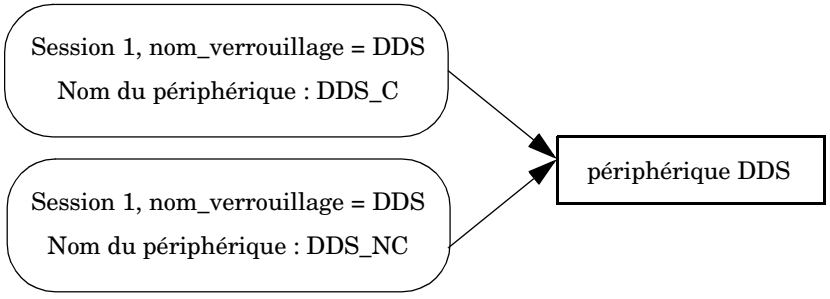
Lorsque vous spécifiez un périphérique utilisé pour la sauvegarde, vous pouvez indiquer un nom de périphérique dans une spécification de sauvegarde, et un autre nom pour le même périphérique physique dans une autre spécification de sauvegarde. Selon la planification des sauvegardes, il se peut que Data Protector essaie d'utiliser le même périphérique physique dans le cadre de sessions de sauvegarde différentes, créant ainsi un conflit.

Prévention des conflits

Afin d'éviter ce type de conflit, spécifiez un nom de verrouillage virtuel dans chaque configuration de périphérique. Data Protector s'assure que les périphériques ont le même nom de verrouillage et évite tout conflit.

Supposons qu'un périphérique autonome DDS ait été configuré comme périphérique compressé sous le nom DDS_C et comme périphérique non compressé sous le nom DDS_NC, comme indiqué à la figure 3-11. Spécifiez le même nom de verrouillage, DDS, pour les deux périphériques.

Figure 3-11 Verrouillage de périphérique et noms de périphérique



Périphériques autonomes

Que sont les périphériques autonomes ?

Les périphériques autonomes sont des périphériques disposant d'un lecteur qui lit/écrit sur un support à la fois.

Les périphériques autonomes sont utilisés pour des sauvegardes à petite échelle ou pour des sauvegardes spéciales. Lorsque le support est saturé, l'opérateur doit le remplacer manuellement par un nouveau support pour que la sauvegarde puisse continuer.

Data Protector et les périphériques autonomes

Lorsque vous avez relié un périphérique au système, vous devez recourir à l'interface utilisateur Data Protector pour le configurer et pouvoir l'utiliser dans Data Protector. Pour ce faire, vous devez installer un Agent de support Data Protector sur le système auquel le périphérique est connecté. Data Protector peut détecter et configurer automatiquement la plupart des périphériques autonomes.

Pendant une sauvegarde, Data Protector émet une demande de montage lorsque le support d'un périphérique est saturé. L'opérateur doit alors remplacer le support pour que la sauvegarde puisse continuer.

Que sont les chaînes de périphériques ?

Data Protector vous permet de définir plusieurs périphériques autonomes en tant que chaîne de périphériques. Lorsqu'un support est plein dans un périphérique, la sauvegarde se poursuit automatiquement sur le support du périphérique suivant dans la chaîne de périphériques.

Les chaînes de périphériques permettent de lancer des sauvegardes sans surveillance axées sur plusieurs périphériques autonomes, évitant ainsi à l'utilisateur de devoir insérer/éjecter manuellement des supports lorsque les supports utilisés sont pleins.

Périphériques chargeurs

Les périphériques chargeurs, similaires aux chaînes de périphériques, contiennent un certain nombre de supports à utiliser dans un ordre séquentiel. Lorsqu'un support est plein, le support suivant est chargé et utilisé pour la sauvegarde.

Petits périphériques de magasin

Que sont les périphériques de magasin ?

Les périphériques de magasin regroupent un certain nombre de supports dans une même unité appelée magasin. Data Protector considère le magasin comme un support unique. Un magasin possède une plus grande capacité qu'un support unique et il est plus facile à gérer que plusieurs supports séparés. Pour obtenir la liste des périphériques pris en charge, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

Data Protector et les périphériques de magasin

Data Protector permet d'effectuer des tâches de gestion de supports sur un magasin, telle que l'émulation d'un support unique. Différentes vues des magasins et des supports sont fournies à cet effet.

Vous pouvez également utiliser un périphérique de magasin en tant que bibliothèque standard, sans tenir compte de la fonction Data Protector de prise en charge des magasins. Data Protector peut détecter et configurer automatiquement les périphériques de magasin.

Nettoyage de lecteurs encrassés

Data Protector peut utiliser des bandes nettoyantes pour nettoyer automatiquement les magasins et autres périphériques lorsqu'ils sont encrassés.

Grandes bibliothèques

Que sont les périphériques de bibliothèque ?

Les périphériques de bibliothèque sont des périphériques automatisés, également appelés chargeurs automatiques, échangeurs ou bibliothèques de bandes magnéto-optiques. Dans Data Protector, la plupart des bibliothèques sont configurées comme bibliothèques SCSI. Elles contiennent un certain nombre de cartouches au niveau d'un référentiel de périphérique et sont équipées dans certains cas de différents lecteurs permettant l'écriture sur plusieurs supports à la fois.

Un périphérique de bibliothèque type dispose d'un ID SCSI pour chacun de ses lecteurs et un pour le mécanisme robotique de bibliothèque qui assure le transfert des supports entre les emplacements et les lecteurs. Par exemple, une bibliothèque équipée de quatre lecteurs possède cinq ID SCSI, quatre pour les lecteurs et un pour le mécanisme robotique.

Data Protector prend également en charge les bibliothèques silo, telles que HP StorageWorks, StorageTek/ACSLS et ADIC/GRAU AML. Pour obtenir la liste des périphériques pris en charge, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

Gestion des supports

L'interface utilisateur Data Protector fournit une vue de bibliothèque spéciale, qui simplifie la gestion des périphériques de bibliothèque.

Les supports d'un grand périphérique de bibliothèque peuvent tous appartenir au même pool de supports Data Protector ou être répartis sur plusieurs pools.

Configuration d'une bibliothèque

Lorsque vous configurez un périphérique, vous définissez la plage d'emplacements que vous voulez attribuer à Data Protector. Cela permet de partager la bibliothèque avec d'autres applications. Les emplacements attribués peuvent contenir des supports vierges (neufs), des supports Data Protector ou d'autres types de support. Data Protector vérifie les supports dans les emplacements et affiche des informations les concernant dans la vue de la bibliothèque. Cela vous permet de visualiser tous les types de support, y compris ceux qui ne sont pas utilisés par Data Protector.

Taille d'une bibliothèque

Les points suivants peuvent vous aider à estimer la taille de la bibliothèque dont vous avez besoin :

- Déterminez si les supports doivent être répartis sur plusieurs sites ou regroupés sur un même site.
- Calculez le nombre de supports requis. Reportez-vous à la section "Mise en œuvre d'une stratégie de rotation des supports" à la page 146.

Partage d'une bibliothèque avec d'autres applications

Il est possible de partager un périphérique de bibliothèque avec d'autres applications stockant des données sur des supports de ce périphérique.

Vous pouvez sélectionner les lecteurs de la bibliothèque devant être utilisés dans Data Protector. Supposons que vous utilisiez une bibliothèque comprenant quatre lecteurs : vous pouvez dans ce cas décider d'utiliser deux de ces lecteurs dans Data Protector.

Vous pouvez sélectionner les emplacements de la bibliothèque devant être gérés dans Data Protector. Supposons que vous utilisiez une bibliothèque comprenant 60 emplacements : vous pouvez dans ce cas décider d'utiliser les emplacements 1 à 40 dans Data Protector. Les autres emplacements peuvent être utilisés et contrôlés par une autre application.

Le partage d'une bibliothèque entre plusieurs applications est fondamental dans le cas d'une grande bibliothèque HP et d'une bibliothèque silo (StorageTek/ACSLS, ADIC/GRAU AML, etc.).

Logements d'insertion/éjection

Les périphériques de bibliothèque disposent de logements d'insertion/éjection spéciaux que l'opérateur peut utiliser pour insérer des supports dans le périphérique et les en éjecter. Selon les périphériques, plusieurs compartiments d'insertion/d'éjection peuvent exister. Dans le cas d'un logement d'insertion/éjection unique, les supports sont insérés un par un, alors que dans le cas de compartiments multiples, il est possible d'utiliser un nombre spécifique de compartiments pour effectuer l'opération d'insertion/d'éjection en une seule étape.

Data Protector permet d'insérer/éjecter plusieurs supports en une seule étape. Par exemple, vous pouvez sélectionner 50 compartiments dans le périphérique et éjecter tous les supports en une seule opération. Data Protector éjecte automatiquement les supports dans le bon ordre pour que l'opérateur puisse retirer les supports du logements d'insertion/éjection.

Pour plus d'informations, reportez-vous à la documentation fournie avec votre périphérique.

Support de code-barres

Data Protector prend en charge les périphériques de bibliothèque équipés d'un lecteur de code-barres. Dans ces périphériques, chaque support dispose d'un code-barres l'identifiant de manière unique.

Avantages des codes-barres

Les fonctions d'identification des supports, d'étiquetage et de détection de bande nettoyante donnent de meilleurs résultats lorsque Data Protector utilise les codes-barres.

- L'analyse des codes-barres des supports contenus dans un référentiel de périphérique permet d'accélérer la procédure : en effet, il n'est pas nécessaire que Data Protector charge les supports dans un lecteur et lise leur en-tête.
- Le code-barre est automatiquement lu par Data Protector et permet d'identifier le support.
- Une bande nettoyante est automatiquement détectée si elle dispose d'un préfixe de code-barres CLN.
- Le code-barres fournit un ID unique à chaque support dans la base de données IDB. Vous ne pouvez pas avoir deux codes-barres identiques dans votre environnement.

CONSEIL

Le cas échéant, vous pouvez utiliser le code-barres comme étiquette du support pendant l'initialisation du support.

Prise en charge des bandes nettoyantes

HP Data Protector permet le nettoyage automatique des bandes sur la plupart des périphériques prenant en charge les bandes nettoyantes. Une bande nettoyante est utilisée automatiquement par Data Protector lorsqu'un événement "lecteur encrassé" provenant du périphérique est détecté.

- Dans les bibliothèques SCSI, il est possible de définir quels emplacements contiendront une bande nettoyante.
- Dans le cas de périphériques disposant d'un lecteur de code-barres, Data Protector reconnaît automatiquement les codes-barres de la bande nettoyante, à condition qu'ils contiennent le préfixe CLN.
- Pour les périphériques sans bande nettoyante, une détection de lecteur encrassé entraîne une demande de nettoyage affichée dans la fenêtre du moniteur de session. L'opérateur doit ensuite nettoyer le périphérique manuellement.

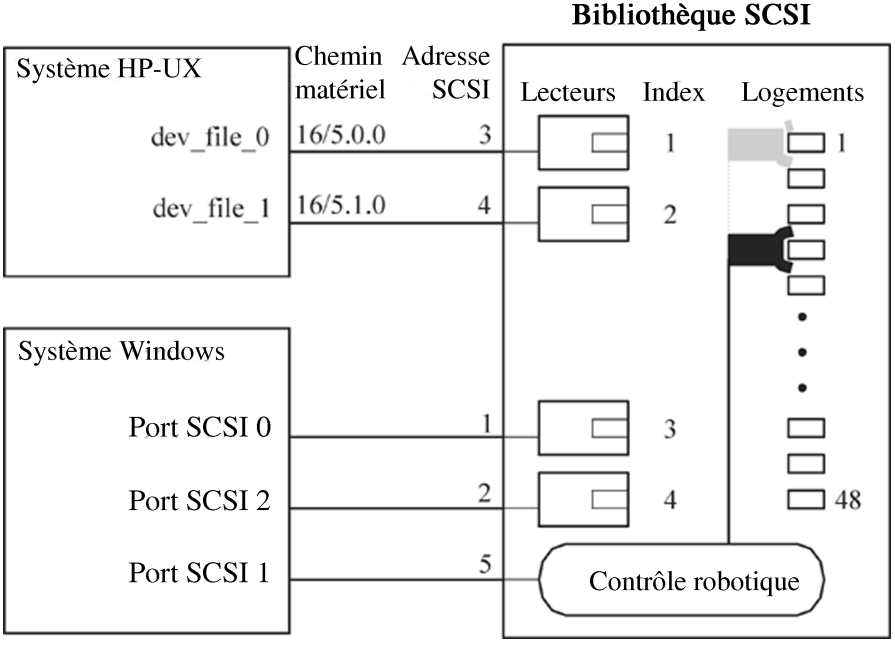
  Vous ne pouvez pas continuer votre sauvegarde si vous ne nettoyez pas le lecteur : la sauvegarde risque d'échouer car les données peuvent ne pas être correctement écrites ou stockées sur le support.

Partage d'une bibliothèque entre plusieurs systèmes

Qu'est-ce que le partage de bibliothèques ?

Le partage de périphériques vous permet de relier plusieurs lecteurs d'une bibliothèque physique à différents systèmes. Ces systèmes peuvent alors effectuer des sauvegardes locales dans la bibliothèque. Les performances de la sauvegarde en sont améliorées de manière significative et le trafic réseau réduit. Pour partager la bibliothèque, les lecteurs de la bibliothèque doivent pouvoir être reliés à des bus SCSI séparés. Dans le cas de bibliothèques hautes performances, le partage est particulièrement utile puisqu'il permet au lecteur de recevoir des données en mode continu à partir de plusieurs systèmes, améliorant ainsi les performances. Data Protector redirige en interne les commandes robotiques vers le système qui gère le robot.

Figure 3-12 Connexion de lecteurs à plusieurs systèmes



Protocoles de contrôle et Agents de support Data Protector

Les lecteurs présents dans la bibliothèque doivent être capables de se connecter physiquement à différents systèmes équipés d'un Agent de support Data Protector (l'Agent général de supports ou l'Agent de support NDMP).

Data Protector permet d'utiliser deux types de protocole pour le contrôle des lecteurs :

- SCSI - pour les lecteurs SCSI ou Fibre Channel.

  Le protocole est mis en œuvre à la fois dans l'Agent général de supports et dans l'Agent de support NDMP.

- NDMP - pour les lecteurs dédiés NDMP.

  Ce protocole est mis en œuvre uniquement dans l'Agent de support NDMP.

D'autre part, il existe quatre types de protocoles utilisés pour le contrôle du robot de bibliothèque.

- ADIC/GRAU - pour le robot de bibliothèque ADIC/GRAU

- StorageTek ACS - pour le robot de bibliothèque ASC StorageTek
- SCSI - pour le robot d'autres bibliothèques
- NDMP - pour le robot NDMP

Les quatre protocoles de contrôle du robot de bibliothèque sont mis en œuvre à la fois dans l'Agent général de supports et dans l'Agent de support NDMP.

Contrôle des lecteurs

Tout système client Data Protector configuré pour contrôler un lecteur dans une bibliothèque (quels que soient le protocole de contrôle du lecteur et la plate-forme utilisés) peut communiquer avec n'importe quel système client Data Protector configuré pour contrôler le robot dans la bibliothèque (quels que soient le protocole de contrôle des robots et la plate-forme utilisés). Il est ainsi possible de partager les fichiers dans n'importe quelle bibliothèque gérée parmi les systèmes clients Data Protector sur plusieurs plates-formes utilisant différents protocoles de robot et lecteur. L'Agent de support NDMP ne doit être installé que sur des systèmes client qui contrôlent la sauvegarde de données d'un serveur NDMP (systèmes client configurés pour les lecteurs dédiés NDMP). Dans tous les autres cas, les deux Agents de support Data Protector sont interchangeables.

Le tableau 3-1 présente l'Agent de support Data Protector (l'Agent général de supports ou l'Agent de support NDMP) requis sur les systèmes clients configurés pour le contrôle des lecteurs d'une bibliothèque dotée de lecteurs partagés entre plusieurs systèmes clients.

Tableau 3-1 Agent de support Data Protector requis pour le contrôle des disques

	Protocole de contrôle des données	
	NDMP	**SCSI**
Protocole de contrôle des robots (ADIC/GRAU, StorageTek ACS, SCSI ou NDMP)	Agent de support NDMP	Agents de support NDMP ou Agent général de supports

Contrôle robotique

Un système client Data Protector contrôlant le robot de bibliothèque peut être doté de l'Agent général de supports ou l'Agent de support NDMP, quel que soit le type de protocole de lecteur (NDMP ou SCSI) utilisé avec les lecteurs dans la bibliothèque.

Le tableau 3-2 présente l'Agent de support Data Protector (l'Agent général de support ou l'Agent de support NDMP) requis sur un système client configuré pour le contrôle des robots d'une bibliothèque dotée de lecteurs partagés entre plusieurs systèmes clients.

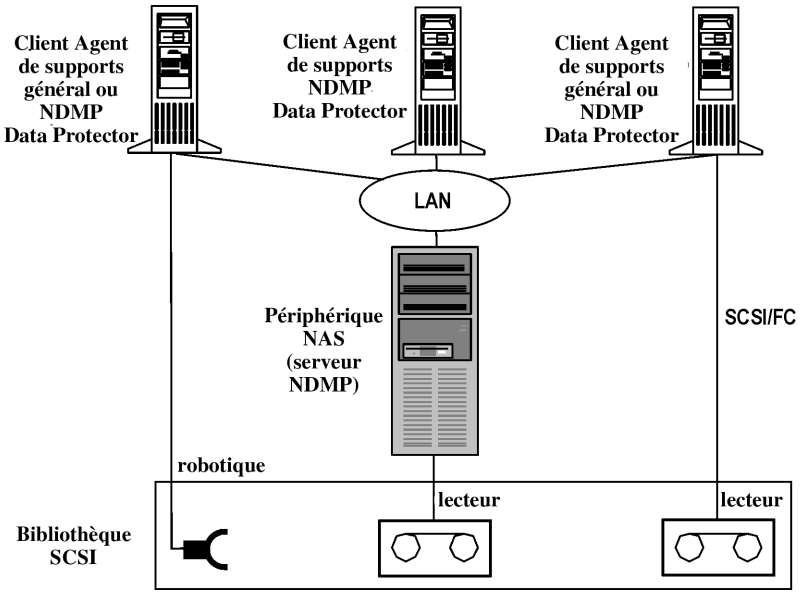
Tableau 3-2 Agent de support Data Protector requis pour le contrôle des robots

	Protocole de contrôle des robots			
	ADIC/GRAU	**StorageTek ACS**	**SCSI**	**NDMP**
Protocole de contrôle des lecteurs (NDMP ou SCSI)	Agents de support NDMP ou Agent général de supports	Agents de support NDMP ou Agent général de supports	Agents de support NDMP ou Agent général de supports	Agents de support NDMP ou Agent général de supports

Exemples de configurations

Les figures 3-13 à 3-15 présentent des contrôles de configurations de lecteurs partagés dans les bibliothèques et de distributions des Agents de support Data Protector dans les configurations en question.

Figure 3-13 **Partage d'une bibliothèque SCSI (robot relié à un système client Data Protector)**

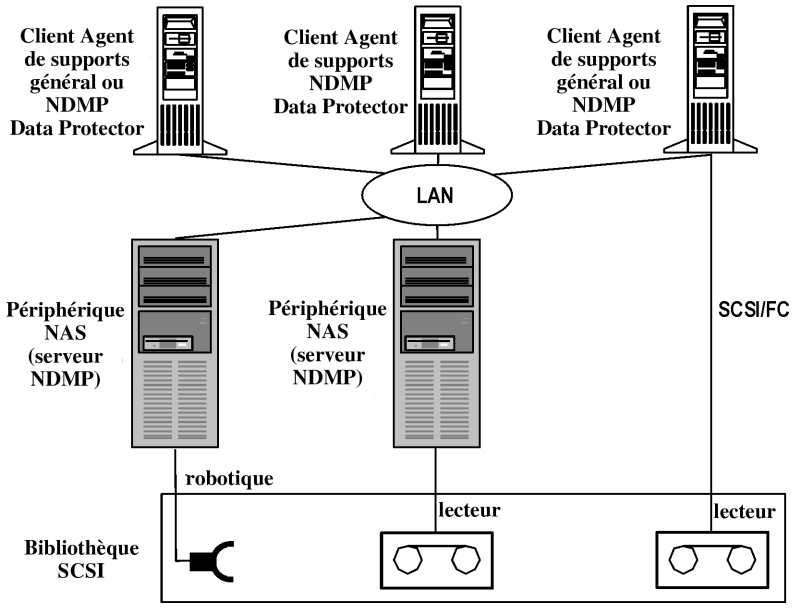


La figure 3-13 présente une bibliothèque SCSI, ainsi que ses robots connectés au système client Data Protector et configurés sur ce dernier, sur lequel l'Agent général de supports ou l'Agent de support NDMP est installé. Le protocole de contrôle du robot SCSI est utilisé par l'Agent général de supports ou l'Agent de support NDMP sur le client. Le système client Data Protector auquel le robot est connecté peut également être relié à un ou plusieurs lecteurs.

Le lecteur dédié NDMP de la bibliothèque est configuré sur le système client Data Protector, sur lequel l'Agent de support NDMP est installé. L'Agent de support NDMP utilise le protocole de contrôle de lecteurs NDMP sur le client.

Un autre lecteur de la bibliothèque est relié au système client Data Protector et configuré sur ce dernier, sur lequel l'Agent général de supports ou l'Agent de support NDMP est installé. Le protocole de contrôle du lecteur SCSI est utilisé par l'Agent général de supports ou l'Agent de support NDMP sur le client.

Figure 3-14 **Partage d'une bibliothèque SCSI (robot relié à un serveur NDMP)**



La figure 3-14 présente une bibliothèque SCSI, ainsi que ses robots connectés à un serveur NDMP et configurés sur le système client Data Protector, sur lequel l'Agent général de supports ou l'Agent de support NDMP est installé. Le protocole de contrôle du robot SCSI est utilisé par l'Agent général de supports ou l'Agent de support NDMP sur le client. Le serveur NDMP auquel le robot est connecté peut également être relié à un ou plusieurs lecteurs.

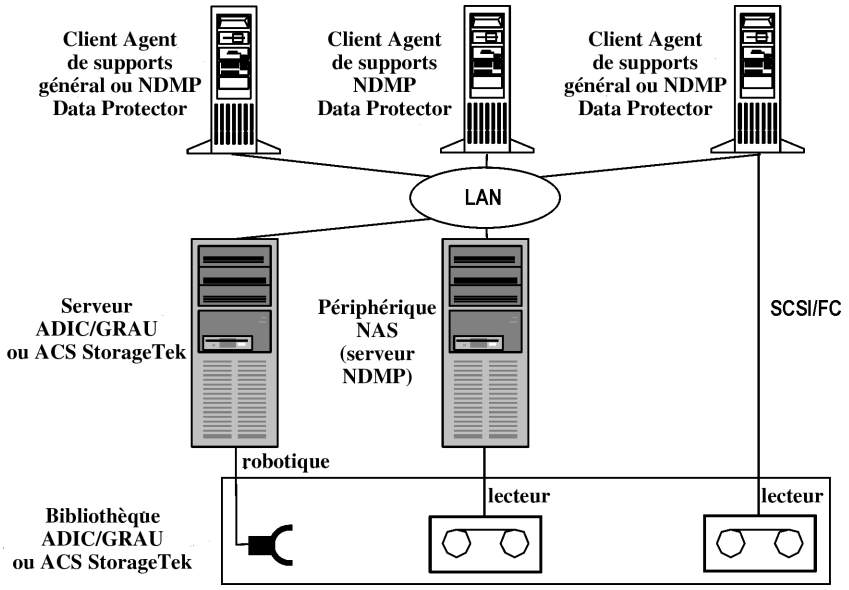
IMPORTANT

Si le serveur NDMP doté du robot est également relié à un lecteur dédié NDMP, le système client Data Protector sur lequel le robot et le lecteur dédié NDMP sont configurés, peut être pourvu uniquement de l'Agent de support NDMP, puisque le protocole de contrôle de lecteurs NDMP est utilisé pour le lecteur dédié NDMP.

Le lecteur dédié NDMP de la bibliothèque est configuré sur le système client Data Protector, sur lequel l'Agent de support NDMP est installé. L'Agent de support NDMP utilise le protocole de contrôle de lecteurs NDMP sur le client.

Un autre lecteur de la bibliothèque est relié au système client Data Protector et configuré sur ce dernier, sur lequel l'Agent général de supports ou l'Agent de support NDMP est installé. Le protocole de contrôle du lecteur SCSI est utilisé par l'Agent général de supports ou l'Agent de support NDMP sur le client.

Figure 3-15 Partage d'une bibliothèque ADIC/GRAU ou ACS StorageTek



La figure 3-15 présente une bibliothèque ADIC/GRAU ou ACS StorageTek, ainsi que ses robots connectés à un serveur ADIC/GRAU ou ACS StorageTek et configurés sur le système client Data Protector sur lequel l'Agent général de supports ou l'Agent de support NDMP est installé. Le protocole de contrôle du robot ADIC/GRAU est utilisé par l'Agent général de supports ou l'Agent de support NDMP sur le client. Le serveur ADIC/GRAU ou ACS StorageTek ACS peut également être connecté à un ou plusieurs lecteurs.

Le lecteur dédié NDMP de la bibliothèque est configuré sur le système client Data Protector, sur lequel l'Agent de suppor NDMP est installé. L'Agent de support NDMP utilise le protocole de contrôle de lecteurs NDMP sur le client.

Un autre lecteur de la bibliothèque est relié au système client Data Protector et configuré sur ce dernier, sur lequel l'Agent général de supports ou l'Agent de support NDMP est installé. Le protocole de contrôle du lecteur SCSI est utilisé par l'Agent général de supports ou l'Agent de support NDMP sur le client.

Data Protector et Storage Area Networks

Le lieu et le mode de stockage des données utilisés dans votre entreprise peuvent avoir d'importantes répercussions sur votre activité. Pour la plupart des sociétés, l'information prend une importance croissante. Les utilisateurs doivent pouvoir accéder à des téraoctets de données à travers le réseau. La technologie Fibre Channel basée sur SAN mise en oeuvre par Data Protector vous offre la solution de stockage des données dont vous avez besoin.

Storage Area Networks

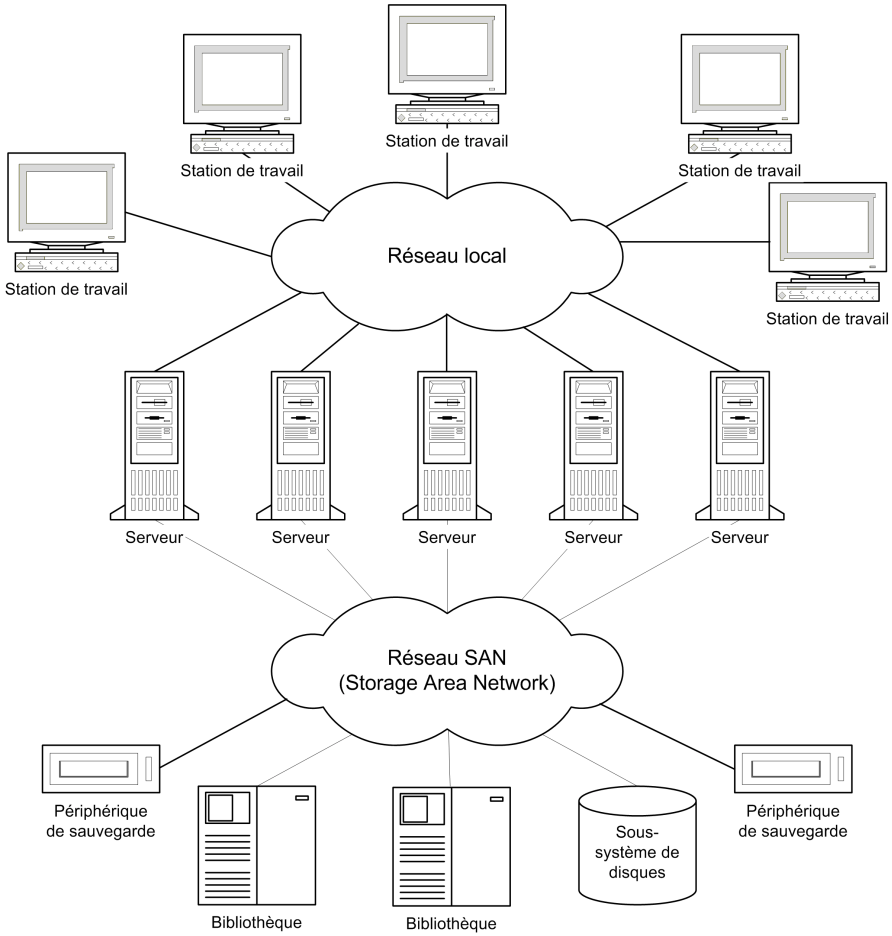
Un Storage Area Network (SAN), illustré à la figure 3-16, représente une nouvelle approche de stockage en réseau, séparant la gestion de stockage de la gestion de serveur grâce à un réseau entièrement dédié au stockage.

Un SAN permet l'*interconnectivité* de l'ensemble des ressources du réseau : les périphériques peuvent ainsi être partagés entre plusieurs systèmes client et le trafic de données ainsi que la disponibilité des périphériques sont améliorés.

Le concept SAN permet l'échange de données entre plusieurs serveurs et périphériques de stockage de données. Les serveurs peuvent accéder directement aux données de tout périphérique et n'ont pas besoin de transférer les données par le réseau local classique. Un SAN se compose de serveurs, de périphériques de sauvegarde, de baies de disques et d'autres nœuds, tous reliés par une connexion réseau rapide (généralement Fibre Channel). Ce réseau supplémentaire permet de décharger le réseau local classique, les opérations de stockage étant prises en charge par un réseau séparé.

La fonctionnalité de sauvegarde directe de Data Protector est une mise en application pratique de la technologie SAN et Fibre Channel.

Figure 3-16 Storage Area Network



Fibre Channel

Fibre Channel est une norme ANSI pour l'interconnexion informatique à grande vitesse. Utilisant des câbles à fibre optique ou en cuivre, cette technologie permet la transmission bidirectionnelle de fichiers de données volumineux à une vitesse pouvant atteindre 4,25 gigabits par seconde, et peut être déployée entre des sites distants compris dans un

périmètre de 30 km. La technologie Fibre Channel est à ce jour la solution la plus fiable et la plus performante pour le stockage, le transfert et la récupération des informations.

La technologie Fibre Channel relie les nœuds au moyen de trois topologies physiques différentes (présentant certaines variantes) :

- Point à point
- En boucle
- Commutée

Les topologies Fibre Channel point à point, en boucle et commutées peuvent être combinées pour répondre au mieux à vos exigences de connectivité et de croissance.

Reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector* ou consultez le site Web http://www.openview.hp.com/products/datapro/spec_0001.html pour obtenir une liste des configurations prises en charge.

Topologie point à point

Cette topologie permet la connexion de deux nœuds, généralement un serveur et un périphérique de sauvegarde. Les principaux avantages sont l'amélioration des performances et l'augmentation des distances entre les nœuds.

Topologie en boucle

La topologie en boucle s'appuie sur la norme Fibre Channel Arbitrated Loop (FC-AL), qui permet de connecter jusqu'à 126 nœuds. Les nœuds comprennent les serveurs, les périphériques de sauvegarde, les concentrateurs et les commutateurs. Tout nœud d'une boucle peut communiquer avec un autre nœud de la boucle, et tous les nœuds partagent la même bande passante. Une boucle FC-AL est généralement mise en œuvre à l'aide d'un concentrateur FC-AL avec substitution automatique de port. La substitution automatique de port permet le branchement de nœuds à chaud à l'intérieur de la boucle.

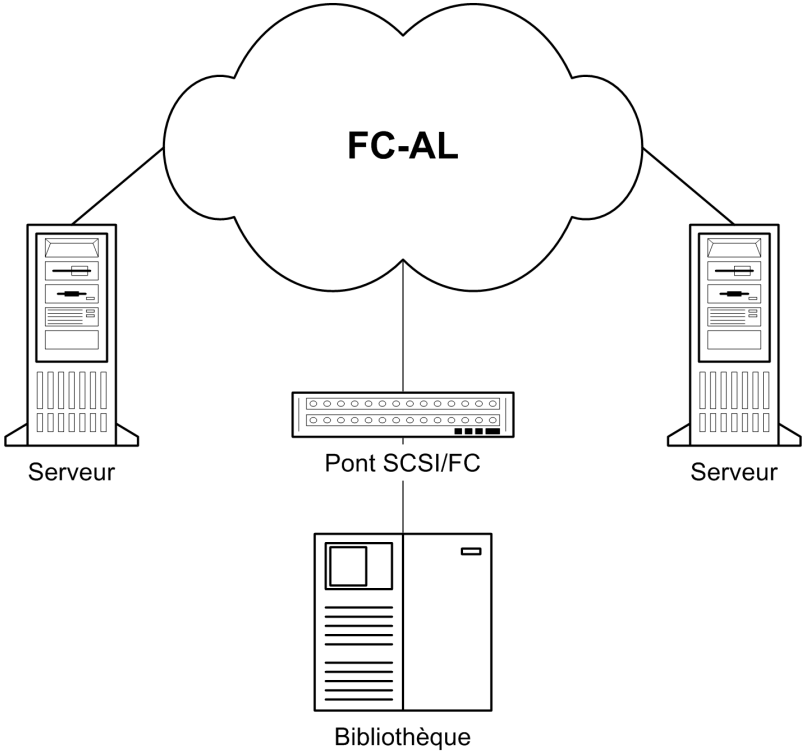
LIP

Une primitive LIP (Loop Initialization Primitive - Protocole) peut être déclenchée pour plusieurs raisons, la plus courante étant l'apparition d'un nouveau périphérique. Le nouveau périphérique peut être un périphérique utilisé précédemment ayant été allumé ou un périphérique actif ayant été déplacé d'un port du commutateur à un autre.

Une occurrence LIP peut provoquer une interruption inopportune d'une procédure en cours sur SAN, par exemple une opération de sauvegarde sur bande. Le bus SCSI reliant la passerelle SCSI/FC et le nœud (périphérique SCSI) est réinitialisé. Reportez-vous à la figure 3-17.

Lors d'une sauvegarde ou d'une restauration, la réinitialisation du bus SCSI est enregistrée comme erreur d'écriture. Data Protector abandonne toutes les opérations en cas d'erreur d'écriture. Dans le cas de sauvegardes, il est recommandé de copier les données déjà sauvegardées sur un support, puis de reformater le support et de redémarrer la sauvegarde.

Figure 3-17 Loop Initialization Protocol



Topologie commutée

La topologie commutée fournit une interconnectivité entre tous les nœuds reliés à un commutateur. Les commutateurs sont faciles à installer et à utiliser, le protocole Fibre Channel permettant l'autoconfiguration et l'autogestion. Les commutateurs détectent automatiquement les équipements connectés (nœuds, concentrateurs FC-AL ou tout autre commutateur FC) et s'autoconfigurent en conséquence. Les commutateurs fournissent aux nœuds connectés une bande passante proportionnée. La topologie commutée permet de brancher les nœuds à chaud.

REMARQUE Le branchement à chaud correspond à certaines capacités du protocole, telles que la réinitialisation, le rétablissement des communications, etc. N'oubliez pas que les transferts de données en cours sont interrompus pendant le branchement à chaud et que certains périphériques, tels que les périphériques à bande, ne gèrent pas cette fonctionnalité. Le fait de connecter ou de déconnecter les nœuds d'une boucle risque d'interrompre la procédure de sauvegarde ou de restauration et de faire échouer l'opération. Pour connecter ou déconnecter les nœuds d'une boucle, vérifiez qu'aucune sauvegarde ou restauration n'utilise le matériel associé.

Partage de périphériques dans SAN

Data Protector prend en charge le concept SAN dans la mesure où il permet à plusieurs systèmes de partager des périphériques de sauvegarde dans l'environnement SAN. Le même périphérique physique est accessible à partir de plusieurs systèmes. Tout système peut donc effectuer une sauvegarde locale sur ce périphérique ou tout autre périphérique. Les données étant transférées via le SAN, les sauvegardes n'ont pas besoin de bande passante sur votre réseau local classique. Ce type de sauvegarde est parfois appelé "sauvegarde indépendante du réseau local". Les performances de la sauvegarde sont améliorées, la technologie Fibre Channel basée sur SAN offrant un débit supérieur à celui des technologies de réseau local.

Vous devez empêcher les systèmes dotés de plusieurs ordinateurs d'écrire sur le même périphérique en même temps. La situation est encore plus complexe lorsque les périphériques sont utilisés par plusieurs applications. L'accès aux périphériques doit être synchronisé entre tous les systèmes impliqués. Cette opération est effectuée grâce à des mécanismes de verrouillage.

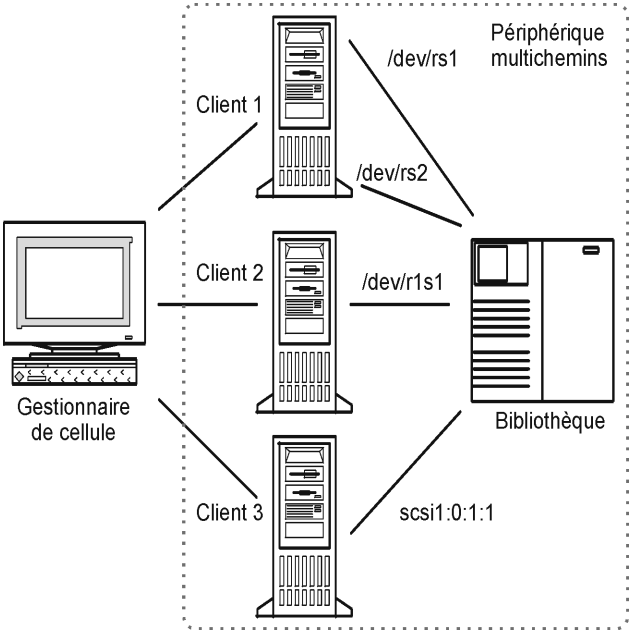
La technologie SAN représente un excellent moyen de gérer le robot d'une bibliothèque à partir de plusieurs systèmes. Elle vous offre la possibilité de gérer les robots à partir d'un même système (classique) ou d'autoriser chaque système utilisant la bibliothèque d'accéder directement aux robots, à condition que les requêtes robotiques soient synchronisées entre tous les systèmes impliqués.

Configuration de plusieurs chemins vers des périphériques physiques

Un périphérique dans un environnement SAN est généralement connecté à différents clients et il est ainsi possible d'y accéder via plusieurs chemins, à savoir des noms de client et des adresses SCSI (fichiers de périphérique sur UNIX). Data Protector peut utiliser l'un de ces chemins. Vous pouvez configurer tous les chemins sur un périphérique physique en tant que périphérique logique unique - **périphérique multichemins**.

Par exemple, un périphérique est connecté à `client1` et configuré en tant que `/dev/rs1` et `/dev/rs2`, sur `client2` en tant que `/dev/r1s1` et sur `client3` en tant que `scsi1:0:1:1`. Quatre chemins distincts permettent donc d'y accéder : `client1:/dev/rs1`, `client1:/dev/rs2`, `client2:/dev/r1s1` et `client3:scsi1:0:1:1`. Un périphérique multichemins contient par conséquent les quatre chemins vers ce périphérique à bandes.

Figure 3-18 Exemple de configuration multichemins



Pourquoi utiliser plusieurs chemins ?

Les versions antérieures de Data Protector permettaient d'accéder à chaque périphérique à partir d'un seul client. Pour remédier à ce problème, plusieurs périphériques logiques devaient être configurés pour un périphérique physique utilisant un nom de verrouillage. Ainsi, si vous utilisiez des noms de verrouillage pour la configuration de l'accès à partir de différents systèmes vers un seul périphérique physique, vous deviez configurer tous les périphériques sur chaque système. Par exemple, si vous disposez de 10 clients connectés à un seul périphérique, vous devez configurer 10 périphériques avec le même nom de verrouillage. Cette version de Data Protector vous permet de simplifier la configuration en configurant un seul périphérique multichemins pour l'ensemble des chemins.

Les périphériques multichemins augmentent la résilience des systèmes. Data Protector essaiera d'utiliser le premier chemin défini. Si tous les chemins sur un client sont inaccessibles, Data Protector essaiera d'utiliser les chemins sur le client suivant. La session échoue uniquement lorsque aucun des chemins répertoriés n'est disponible.

Sélection des chemins

Pendant une session de sauvegarde, les chemins sont sélectionnés dans l'ordre défini au cours de la configuration, excepté si :

- Un client favori est sélectionné dans la spécification de sauvegarde. Dans ce cas, le client favori est utilisé en premier.
- L'accès direct à la bibliothèque est activé. Dans ce cas, les chemins locaux (chemins figurant sur le client destinataire) sont utilisés en premier.

Lors de la restauration, les chemins sont sélectionnés dans l'ordre suivant :

- Chemins locaux
- Chemins utilisés pour la sauvegarde
- Autres chemins disponibles

Compatibilité en amont

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 utiliser la nouvelle fonctionnalité multichemins, les périphériques doivent être reconfigurés en tant que périphériques multichemins.

Verrouillage de périphérique

Le verrouillage de périphérique concerne les cas dans lesquels plusieurs applications utilisent le même périphérique et ceux dans lesquels Data Protector utilise un périphérique pour l'envoi de données et de commandes vers celui-ci à partir de plusieurs systèmes. Le but du verrouillage est de s'assurer qu'un seul système communique avec un périphérique partagé entre plusieurs systèmes.

Verrouillage de périphérique et applications multiples

Si Data Protector et au moins une autre application doivent utiliser le même périphérique à partir de plusieurs systèmes, le même mécanisme de verrouillage de périphérique (générique) doit être utilisé par chaque application. Ce mécanisme doit pouvoir fonctionner avec plusieurs applications. Ce mode n'est actuellement pas pris en charge par Data Protector. Si cela est nécessaire, des règles de fonctionnement doivent être appliquées pour garantir l'accès exclusif d'une application à tous les périphériques.

Verrouillage de périphérique dans Data Protector

Si Data Protector est la seule application utilisant un lecteur, mais que ce lecteur doit être utilisé par plusieurs systèmes, vous devez utiliser le mécanisme de verrouillage de périphérique.

Si Data Protector est la seule application utilisant le contrôle robotique à partir de plusieurs systèmes, elle gère la procédure en interne à condition que le contrôle de bibliothèque se trouve dans la même cellule que tous les systèmes devant la contrôler. Dans ce cas, la synchronisation de l'accès au périphérique est intégralement gérée en interne par Data Protector.

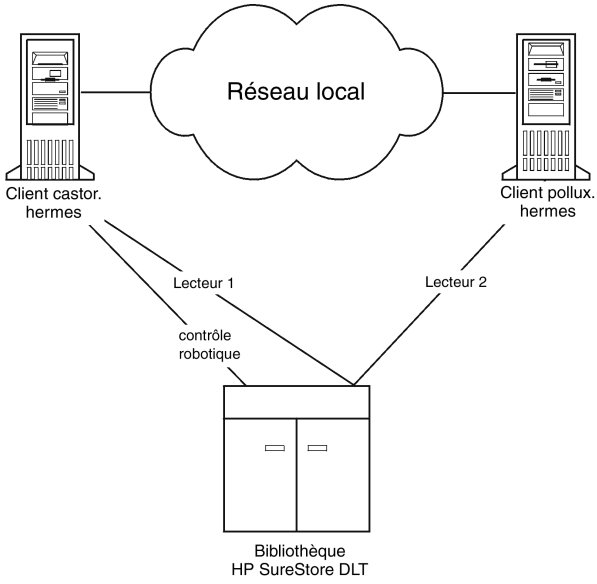
Accès direct et indirect à la bibliothèque

Lors de la configuration de Data Protector associé à un périphérique de bibliothèque SCSI, les systèmes client peuvent accéder au robot de la bibliothèque de deux façons : accès direct et indirect à la bibliothèque.

Accès indirect à la bibliothèque

Cette configuration peut être utilisée à la fois dans SAN et dans les environnements de connexion directe type SCSI. Plusieurs systèmes peuvent accéder au robot de la bibliothèque en envoyant leur demande à un système client disposant d'un accès direct au robot de bibliothèque. C'est ce qu'on appelle l'accès indirect à la bibliothèque. Dans l'exemple illustré à la figure 3-19, deux systèmes client sont reliés à une bibliothèque multilecteurs DLT HP StorageWorks. Le système client `castor` contrôle le robot et le premier lecteur, tandis que le système client `pollux` contrôle le deuxième lecteur. Un Agent de support Data Protector sur `pollux` communique avec un processus en cours d'exécution sur `castor` pour faire fonctionner le robot. Cette fonctionnalité de partage de bibliothèque Data Protector est utilisée automatiquement lorsque les noms d'hôte de la bibliothèque et du lecteur sont différents.

Figure 3-19 Accès indirect à la bibliothèque



Notez que vous ne pouvez pas utiliser de bibliothèque partagée si le système client qui contrôle le robot, `castor` dans notre exemple, échoue.

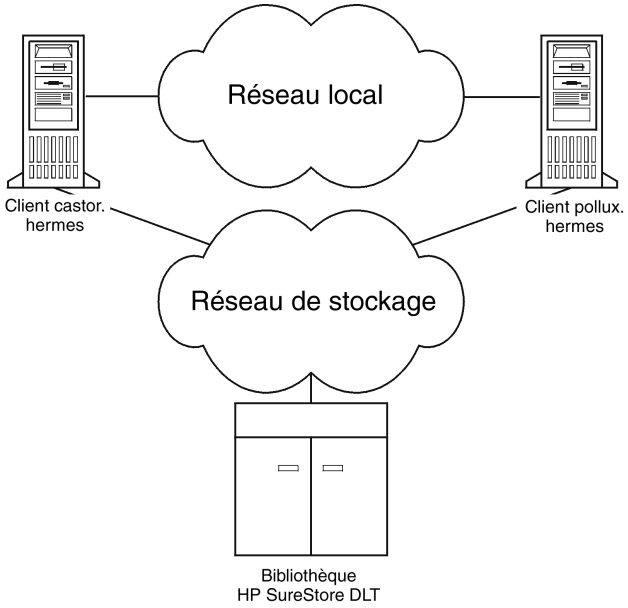
Accès direct à la bibliothèque

Lorsque le concept SAN est utilisé, Data Protector associé à une bibliothèque SCSI peut être configuré pour que chaque système client dispose de son propre accès aux lecteurs et au robot de la bibliothèque. On parle alors d'accès direct à la bibliothèque.

Il n'existe pas de "système client de contrôle" unique pour le robot : l'échec du système contrôlant le robot n'empêche pas les autres systèmes d'utiliser la bibliothèque. Cela est possible sans reconfiguration. Plusieurs systèmes client peuvent être utilisés pour contrôler le robot.

La figure 3-20 montre une bibliothèque multilecteurs DLT HP StorageWorks reliée à deux systèmes client via un SAN. Les deux systèmes client ont accès à la bibliothèque et aux lecteurs. Le protocole SCSI est utilisé pour les communications avec la bibliothèque.

Figure 3-20 Accès direct à la bibliothèque



Partage de périphérique dans les clusters

La gestion de clusters, souvent utilisée en combinaison avec le concept SAN, est basée sur le partage de ressources réseau entre les nœuds (par exemple des noms réseau, des disques et des périphériques à bande).

Les applications compatibles cluster peuvent être lancées à tout moment sur n'importe quel nœud dans un cluster (elles fonctionnent sur des hôtes virtuels). Pour effectuer une sauvegarde locale d'une telle application, vous devez configurer les périphériques disposant de noms d'hôtes virtuels à la place de noms de nœud réels. Configurez autant de périphériques physiques que vous le souhaitez, en utilisant le mécanisme de verrouillage de périphérique "Nom de verrouillage". Pour plus de détails, reportez-vous à la section "Verrouillage de périphérique" à la page 189.

Lecteurs statiques

Les lecteurs statiques sont des périphériques configurés sur un nœud réel dans un cluster. Ils peuvent être utilisés pour sauvegarder des données à partir de systèmes possédant des disques non partagés.

Ils ne sont cependant pas utiles pour les sauvegardes d'applications compatibles cluster, puisque de telles applications peuvent être lancées à partir de n'importe quel nœud du cluster.

Lecteurs flottants

Les lecteurs flottants sont des périphériques configurés sur un hôte virtuel, qui utilisent des noms de système virtuel. Les lecteurs flottants doivent être configurés pour la sauvegarde d'applications compatibles cluster. Cela permet de s'assurer que, quel que soit le nœud du cluster sur lequel l'application s'exécute, Data Protector démarrera toujours un Agent de support sur ce même nœud.

4 Utilisateurs et groupes d'utilisateurs

Description du chapitre

Ce chapitre traite du système de sécurité, des utilisateurs, des groupes d'utilisateurs et des droits utilisateur dans Data Protector.

Il s'organise comme suit :

"Sécurité renforcée pour les utilisateurs Data Protector" à la page 197

"Utilisateurs et groupes d'utilisateurs" à la page 198

Sécurité renforcée pour les utilisateurs Data Protector

Data Protector offre une fonction de sécurité avancée qui permet d'éviter qu'une sauvegarde ou une restauration de données non autorisée soit effectuée. Vous pouvez ainsi interdire l'accès à certaines données aux utilisateurs non autorisés, encoder des données et définir des groupes d'utilisateurs en fonction de leurs responsabilités.

Cette section décrit les différents points de sécurité liés à l'utilisation de Data Protector pour la sauvegarde de données, la restauration de données et le contrôle de l'avancement d'une session de sauvegarde.

Accès à des données sauvegardées

Sauvegarder et restaurer des données revient à copier des données. Il est donc important de limiter l'accès à ces données aux utilisateurs autorisés.

Le système de sécurité Data Protector relatif aux utilisateurs est le suivant :

- Toute personne souhaitant utiliser Data Protector doit être définie comme utilisateur Data Protector.

Visibilité des données sauvegardées

- Seul le propriétaire de la sauvegarde peut visualiser les données qu'il a sauvegardées. Les autres utilisateurs n'ont même pas la possibilité de déterminer si ces données ont été sauvegardées. Par exemple, lorsque l'opérateur de sauvegarde configure une sauvegarde, l'administrateur système et lui sont les seuls autorisés à visualiser et restaurer les données sauvegardées. Vous pouvez rendre des données visibles à d'autres utilisateurs en utilisant l'option `Est public` de Data Protector. Reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector* pour connaître la procédure d'installation.

Utilisateurs et groupes d'utilisateurs

Pour pouvoir utiliser Data Protector, vous devez être ajouté à sa configuration en tant qu'utilisateur Data Protector disposant de certains privilèges. Notez que l'ajout d'un utilisateur ne constitue pas un prérequis pour la sauvegarde du système qu'il utilise.

Les utilisateurs sont réunis au sein de groupes d'utilisateurs ayant des droits spécifiques : par exemple, le droit de contrôler des sessions dans la cellule, de configurer des sauvegardes et de restaurer des fichiers.

Groupes d'utilisateurs prédéfinis

Pour simplifier la configuration des sauvegardes, Data Protector fournit des groupes d'utilisateurs prédéfinis disposant de certains droits d'accès aux fonctionnalités du logiciel. Par exemple, seuls les membres du groupe d'utilisateurs admin peuvent accéder à l'ensemble des fonctionnalités de Data Protector. Par défaut, les opérateurs peuvent lancer et contrôler des sauvegardes.

CONSEIL

Dans les petits environnements, une seule personne suffit pour exécuter toutes les tâches de sauvegarde. Elle doit appartenir au groupe d'utilisateurs admin de Data Protector. Dans ce cas, il n'est pas nécessaire d'ajouter d'autres utilisateurs à la configuration de Data Protector.

En fonction de votre environnement, vous pouvez utiliser les groupes d'utilisateurs Data Protector par défaut, les modifier ou en créer d'autres.

Administrateurs par défaut

Lors de l'installation, les utilisateurs suivants sont automatiquement ajoutés au groupe d'administrateurs Data Protector :

- L'utilisateur "root" UNIX du système Gestionnaire de cellule pour UNIX.
- L'administrateur Windows du système Gestionnaire de cellule pour Windows.
- L'utilisateur ayant installé Data Protector.

Cela permet à ces derniers de configurer et d'utiliser l'intégralité des fonctionnalités de Data Protector.

Utilisation des groupes d'utilisateurs prédéfinis

Les groupes d'utilisateurs suivants sont installés par défaut dans Data Protector :

Tableau 4-1 Groupes d'utilisateurs Data Protector prédéfinis

Groupe d'utilisateurs	Droits d'accès
Admin	Autorisé à configurer Data Protector et à effectuer des sauvegardes, des restaurations et toute autre opération possible.
Opérateur	Autorisé à lancer des sauvegardes et à répondre aux demandes de montage.
Utilisateur final	Autorisé à restaurer ses propres objets. De plus, les utilisateurs peuvent contrôler les demandes de montage et y répondre lors de leurs propres sessions de restauration.

REMARQUE Les fonctions d'administrateur confèrent un pouvoir important. Les membres du groupe d'utilisateurs admin Data Protector disposent de privilèges administrateur système sur tous les clients de la cellule Data Protector.

Droits utilisateur Data Protector

Les utilisateurs de Data Protector disposent des droits utilisateur accordés au groupe auquel ils appartiennent. Par exemple, tous les membres du groupe d'utilisateurs admin disposent des droits du groupe d'utilisateurs admin Data Protector.

Lorsqu'un utilisateur est configuré depuis le domaine Windows, alors que Data Protector s'exécute sur le Gestionnaire de cellule UNIX, la configuration de cet utilisateur doit comporter le nom de domaine ou le groupe de caractères génériques "*".

Pour obtenir une description détaillée des droits utilisateur Data Protector propres à chaque groupe, consultez l'aide en ligne ou le *Guide de l'administrateur de HP OpenView Storage Data Protector*.

5 La base de données interne de Data Protector

Description du chapitre

Ce chapitre décrit l'architecture de la base de données interne (IDB) de Data Protector, son utilisation et son fonctionnement. Vous y trouverez notamment des explications sur les différentes parties de la base de données et leurs enregistrements, des conseils sur la gestion de la croissance et des performances, ainsi que des formules pour calculer la taille de la base. Ces informations sont nécessaires pour pouvoir gérer la configuration et la maintenance de la base de données de manière efficace.

Il s'organise comme suit :

A propos de la base de données IDB

Qu'est-ce que la base de données interne (IDB) de Data Protector ?

La base de données IDB est une base incorporée, qui réside sur le Gestionnaire de cellule et permet d'identifier les données sauvegardées, les supports sur lesquels elles se trouvent, les résultats des sessions de sauvegarde, de restauration, de copie et de gestion des supports ainsi que les périphériques et bibliothèques configurés.

Pourquoi utiliser la base de données IDB ?

La base de données IDB est utilisée pour trois raisons principales :

- Restauration rapide et facile
  Les informations stockées dans la base de données IDB vous permettent de retrouver rapidement les supports requis pour une restauration et d'accélérer ainsi considérablement le processus. Cette base de données vous permet également de parcourir aisément les fichiers et les répertoires à restaurer.
- Gestion de la sauvegarde
  Les informations stockées dans la base de données IDB vous permettent de vérifier comment se sont déroulées les sauvegardes. Vous pouvez également configurer plusieurs rapports au moyen de la fonction de reporting de Data Protector.
- Gestion des supports
  Les informations stockées dans la base de données IDB permettent à Data Protector d'allouer des supports pendant les sessions de sauvegarde et de copie, d'effectuer un suivi des attributs de supports et des emplacements des supports dans les bibliothèques de bandes et de regrouper des supports dans des pools différents.

A propos de la taille et la croissance de la base de données IDB

La base de données IDB peut s'accroître énormément et avoir un impact important sur les performances des sauvegardes et sur le système du Gestionnaire de cellule. Il faut donc que l'administrateur Data Protector comprenne bien le fonctionnement de la base de données IDB et qu'il choisisse, en fonction des besoins, quelles informations y conserver et combien de temps. Son rôle est d'établir un équilibre entre le temps de restauration et la fonctionnalité d'une part, et la taille et la croissance de la base de données IDB d'autre part. Data Protector propose deux paramètres principaux pour vous aider à équilibrer vos besoins : **niveau de journalisation** et **protection de catalogue**. Reportez-vous également à la section "Croissance et performances de la base de données IDB" à la page 216.

Base de données IDB sous Windows Gestionnaire de cellule

Emplacement de la base de données IDB

La base de données IDB dans le Gestionnaire de cellule Windows est située dans le répertoire `<répertoire_Data_Protector>\db40`.

Format de la base de données IDB

La base de données IDB dans le Gestionnaire de cellule Windows stocke toutes les informations textuelles au format UNICODE codé sur deux octets. Cette base de données IDB s'accroît donc un peu plus rapidement que celle du Gestionnaire de cellule UNIX qui stocke les informations au format ASCII.

Le format UNICODE permet de prendre totalement en charge les noms de fichier et les messages localisés dans d'autres langues.

Base de données IDB sous UNIX Gestionnaire de cellule

Emplacement de la base de données IDB

Dans un Gestionnaire de cellule UNIX, la base de données IDB est située dans le répertoire `/var/opt/omni/server/db40`.

Format de la base de données IDB

La base de données IDB dans le Gestionnaire de cellule HP-UX ou Solaris stocke toutes les informations textuelles au format ASCII codé sur un ou plusieurs octets.

Le format ASCII limite la prise en charge des noms de fichier et des messages localisés dans d'autres langues. Lorsque vous sauvegardez des fichiers avec des noms de fichier dans un format codé sur deux octets (UNICODE par exemple), les noms de fichier sont convertis au format ASCII et peuvent ne pas s'afficher correctement dans l'interface Data Protector. Toutefois, les fichiers et les noms de fichier sont restaurés correctement.

Pour plus d'informations, reportez-vous à la section "Internationalisation" à la page B-14.

Base de données IDB dans un environnement Manager-of-Managers

Dans l'environnement Manager-of-Managers (MoM), la base de données centralisée de gestion des supports (CMMDB) vous permet de partager des périphériques et des supports avec plusieurs cellules. Pour plus d'informations sur la fonctionnalité MoM, reportez-vous à la section "Environnements d'entreprise" à la page 15.

Architecture de la base de données IDB

La base de données IDB est constituée des éléments suivants :

- La MMDB (base de données de gestion des supports) ;
- La CDB (base de données catalogue), elle-même divisée en deux parties : les noms de fichier et les autres enregistrements CDB ;
- Les DCBF (fichiers binaires de catalogue des détails) ;
- Les SMBF (fichiers binaires de messages de session) ;
- Les SIBF (fichiers binaires des intégrations sans serveur pour l'intégration NDMP).

Chacun de ces éléments de la base de données IDB stocke des informations spécifiques de Data Protector (enregistrements), agit différemment sur la taille et la croissance de la base de données IDB et se trouve dans un répertoire distinct du Gestionnaire de cellule. Reportez-vous à la figure 5-1.

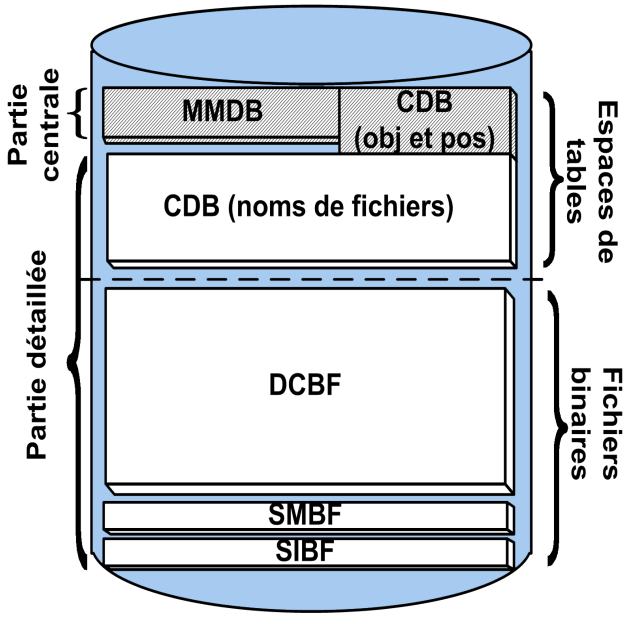
Pour obtenir des informations et des conseils sur l'optimisation de la robustesse par le déplacement de certains répertoires de la base de données IDB, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Technologie sous-jacente

Les parties MMDB et CDB sont mises en œuvre à l'aide d'une base de données intégrée composée d'espaces de table. Celle-ci est contrôlée par le processus du serveur de base de données RDS. Tous les changements apportés à la MMDB et à la CDB sont mis à jour à l'aide des journaux de transaction. Ces derniers sont stockés dans le répertoire `db40\logfiles\syslog`. Les éléments CDB (objets et positions) et MMDB représentent le cœur de la base de données IDB.

Les éléments DCBF, SMBF et SIBF de la base de données IDB sont des fichiers binaires. Les mises à jour se font directement (pas de transaction).

Figure 5-1 **Eléments de la base de données IDB**



Base de données de gestion des supports (MMDB)

Enregistrements MMDB

La base de données de gestion des supports stocke des informations concernant :

- Les périphériques, les bibliothèques, les lecteurs de la bibliothèque et les logements faisant partie de la configuration.
- Les supports Data Protector.
- Les pools et magasins de supports faisant partie de la configuration.

Taille et croissance de la MMDB

La taille de la base de données de gestion des supports n'augmente pas énormément. La plus grande partie de la base de données est généralement occupée par des informations concernant les supports Data Protector. L'espace utilisé est d'environ 30 Mo. Pour plus de détails, reportez-vous à la section "Estimation de la taille de l'IDB" à la page 223.

Emplacement de la MMDB

La MMDB se trouve dans le répertoire suivant :

- Sous Windows : *<répertoire_Data_Protector>*\db40\datafiles\mmdb
- Sous UNIX : /var/opt/omni/server/db40/datafiles/mmdb

Base de données catalogue (CDB)

Enregistrements CDB

La base de données catalogue stocke des informations concernant :

- Les sessions de sauvegarde, de restauration, de copie et de gestion des supports. Il s'agit d'une copie des informations envoyées à la fenêtre Data Protector Monitor.
- Les objets sauvegardés, leurs versions et les copies d'objet.
- Les emplacements des objets sauvegardés sur les supports. Pour chaque objet sauvegardé, Data Protector stocke des informations concernant les supports et les segments de données utilisés pour la sauvegarde ; il en va de même pour les copies d'objet et les mises en miroir d'objet.
- Les chemins d'accès des fichiers sauvegardés (noms de fichier) ainsi que les noms des systèmes client. Les noms de fichier ne sont stockés qu'une fois par système client. Les noms de fichier créés entre les sauvegardes sont ajoutés à la base de données catalogue.

Taille et croissance des noms de fichier

Les noms de fichier représentent la partie la plus importante de la base de données catalogue et celle qui s'accroît le plus vite. Ils occupent en général 20 % de l'ensemble de la base de données.

La croissance de la partie consacrée aux noms de fichier est donc proportionnelle à la croissance et aux variations de l'environnement de sauvegarde, et non au nombre de sauvegardes.

Sur un Gestionnaire de cellule HP-UX ou Solaris, un fichier ou répertoire occupe entre 50 et 70 octets dans la base de données IDB, tandis que sur un Gestionnaire de cellule Windows, il occupe entre 70 et 100 octets.

Les noms de fichier sont stockés dans le fichier fnames.dat et dans certains autres fichiers, selon leur longueur. La taille maximum de chacun de ces fichiers est de 2 Go. Vous êtes informé dès que l'un de ces fichiers commence à être saturé ; cela vous permet d'ajouter de nouveaux fichiers afin d'étendre la taille de la partie noms de fichier de la base de données IDB.

Taille et croissance de la CDB (objets et positions)

Les enregistrements de la base de données catalogue autres que les noms de fichier occupent très peu d'espace dans la base de données IDB. Un environnement de sauvegarde de taille moyenne occupe généralement environ 100 Mo. Pour plus de détails, reportez-vous à la section "Estimation de la taille de l'IDB" à la page 223.

Emplacement de la CDB

La CDB se trouve dans le répertoire suivant :

- Sous Windows : `<répertoire_Data_Protector>\db40\datafiles\cdb`
- Sous UNIX : `/var/opt/omni/server/db40/datafiles/cdb`

Fichiers binaires de catalogue des détails (DCBF)

Informations sur les DCBF

La partie des fichiers binaires de catalogue des détails stocke les informations concernant les versions de fichier. Ces informations se rapportent aux fichiers sauvegardés. Il s'agit notamment de la taille des fichiers, de l'heure de modification, de la protection, des attributs, etc.

Pour chaque support Data Protector utilisé pour une sauvegarde, un fichier binaire DC (catalogue des détails) est créé. Lorsque les informations du support sont écrasées, l'ancien fichier binaire est remplacé par un nouveau.

Taille et croissance des DCBF

Dans un environnement où l'option `Journaliser tout` est fréquemment utilisée pour la sauvegarde des systèmes de fichiers, les DCBF occupent la plus grande partie de la base de données IDB (en général 80 %). Environ 30 octets sont utilisés pour les différentes versions de chaque fichier sauvegardé. Il est possible d'utiliser le niveau de journalisation et la protection de catalogue pour spécifier ce qui est réellement stocké dans la base de données IDB et pour combien de temps. Reportez-vous à la section "Croissance et performances de la base de données IDB : paramètres clés réglables" à la page 217 pour en savoir plus à ce sujet.

Par défaut, il existe un répertoire DC configuré pour les fichiers binaires DC ; il s'agit du répertoire `db40\dcbf`. Sa taille maximum par défaut est de 4 Go. Vous pouvez créer d'autres répertoires DC, les copier sur différents disques du Gestionnaire de cellule et augmenter ainsi la taille de la base de données IDB. Le nombre maximum de répertoires pris en charge par cellule est de 10.

Emplacement des DCBF

Par défaut, les DCBF se trouvent dans le répertoire suivant :

- Sous Windows : `<répertoire_Data_Protector>\db40\dcbf`
- Sous UNIX : `/var/opt/omni/server/db40/dcbf`

Assurez-vous qu'il y a suffisamment d'espace dans le Gestionnaire de cellule. Si ce n'est pas le cas, déplacez le répertoire DC. Vous pouvez créer d'autres répertoires DC et les placer sur différents disques. Ne créez plusieurs répertoires DC que si le nombre de fichiers binaires de DC par support devient très important (plusieurs milliers) ou si vous avez des problèmes d'espace. Pour plus d'informations, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Fichiers binaires de messages de session (SMBF)

Enregistrements SMBF

Les fichiers binaires de messages de session stockent les messages de session générés pendant les sessions de sauvegarde, de restauration, de copie et de gestion des supports. Chaque session génère un fichier binaire. Les fichiers sont regroupés par année et par mois.

Taille et croissance des SMBF

La taille des SMBF dépend des éléments suivants :

- Nombre de sessions exécutées, puisqu'un fichier binaire est créé pour chaque session.
- Nombre de messages dans une session. Un message de session occupe environ 200 octets sur un système Windows et 130 octets sur un système UNIX. Vous pouvez modifier le nombre de messages affichés au moment des opérations de sauvegarde, de restauration et de gestion des supports. Ce paramètre influe également sur le nombre de messages stockés dans la base de données IDB. Pour plus de détails, reportez-vous à la section "Changing the Amount of Messages Shown" à la page 348 du *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Emplacement des SMBF

Les SMBF se trouvent dans le répertoire suivant :

- Sous Windows : `<répertoire_Data_Protector>\db40\msg`
- Sous UNIX : `/var/opt/omni/server/db40/msg`

Vous pouvez déplacer le répertoire en modifiant l'option globale `SessionMessageDir`. Pour obtenir plus d'informations sur le fichier d'options globales de Data Protector, reportez-vous à la section "Global Options File" à la page 565 du *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Fichiers binaires d'intégrations sans serveur (SIBF)

Enregistrements SIBF

Les fichiers SIBF stockent les données de restauration NDMP brutes. Ces données sont nécessaires à la restauration d'objets NDMP.

Taille et croissance des SIBF

Les SIBF n'augmentent pas énormément. Pour plus de détails, reportez-vous à la section "Estimation de la taille de l'IDB" à la page 223. Dans le cas des sauvegardes NDMP, les fichiers SMBF grossissent proportionnellement au nombre d'objets sauvegardés. Environ 3 Ko sont utilisés par objet sauvegardé.

Emplacement des SIBF

Les SIBF se trouvent dans le répertoire suivant :

- Sous Windows : `<répertoire_Data_Protector>\db40\meta`
- Sous UNIX : `/var/opt/omni/server/db40/meta`

Fonctionnement de la base de données IDB

Pendant la sauvegarde

Lorsqu'une session de sauvegarde démarre, un enregistrement de session est créé dans la base de données IDB. Un enregistrement de version d'objet est également créé pour chaque objet et chaque objet miroir de la session. Tous ces enregistrements sont stockés dans la CDB et dotés de plusieurs attributs. Le Gestionnaire de session de sauvegarde met à jour les supports au cours d'une sauvegarde. Tous les enregistrements de support sont stockés dans la MMDB et sont alloués à une sauvegarde en fonction des stratégies définies.

Lorsqu'un segment de données est écrit sur la bande, puis sur un segment de catalogue, un enregistrement d'emplacement de support est stocké dans la CDB pour chaque version d'objet faisant partie de ce segment de données. De plus, le catalogue est stocké dans le fichier binaire de catalogue des détails (DC). Pour chaque support Data Protector, un fichier binaire de catalogue des détails est mis à jour. Le nom du fichier binaire de catalogue des détails est `<IDsupport>_<horodatage>.dat`. Si les données d'un support sont écrasées pendant une sauvegarde, son ancien fichier binaire de catalogue des détails est remplacé par un nouveau.

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

Si la journalisation des transactions est activée, la sauvegarde de la base de données IDB supprime les anciens journaux de transaction et crée de nouveaux journaux nécessaires à la récupération de la base de données IDB.

Pendant la restauration

Lors de la configuration de la restauration, Data Protector réalise une série de requêtes dans les parties CDB et DCBF afin de permettre aux utilisateurs d'explorer les systèmes de fichiers virtuels des données sauvegardées. Ces requêtes d'exploration se divisent en deux étapes. La première consiste à sélectionner un objet spécifique (système de fichiers ou lecteur logique). Si cet objet contient plusieurs versions et/ou copies de sauvegarde stockées, cette opération peut prendre un certain temps car Data Protector analyse les DCBF afin de créer un cache de recherche qui lui permettra d'explorer les répertoires par la suite. La deuxième étape consiste à explorer les répertoires.

Une fois les versions de fichiers spécifiques sélectionnées, Data Protector détermine les supports nécessaires et localise les enregistrements d'emplacement de support utilisés par les fichiers sélectionnés. Ces supports sont ensuite lus par les Agents de support et les données sont envoyées aux Agents de disque qui restaurent les fichiers sélectionnés.

Pendant la copie d'objet

Pendant une session de copie d'objet, les processus qui s'exécutent sont les mêmes que pendant une session de sauvegarde et de restauration. Les données sont lues à partir du support source comme si elles étaient restaurées, puis écrites sur le support cible comme si elles étaient sauvegardées. Une session de copie d'objet entraîne le même effet sur le fonctionnement de la base de données qu'une session de sauvegarde et de restauration. Pour plus d'informations, reportez-vous aux sections "Pendant la sauvegarde" à la page 212 et "Pendant la restauration" à la page 212.

Exportation de support

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

- Tous les enregistrements d'emplacement de support pour ce support sont supprimés de la partie CDB.
- Tous les objets et toutes les copies d'objet qui ne figurent plus sur un autre support sont supprimées de la partie CDB.
- Les sessions obsolètes (dont les supports ont été soit écrasés soit exportés) de plus de 30 jours sont supprimées (cela peut être modifié au moyen de la variable `KeepSession` du fichier d'options globales). Les messages de ces sessions sont également supprimés.
- L'enregistrement du support est supprimé de la partie MMDB et le fichier binaire de catalogue des détails correspondant est supprimé des DCBF.

Suppression du catalogue des détails

Lorsque le catalogue des détails est supprimé pour un support donné, le fichier binaire DC correspondant l'est également. Le même résultat est obtenu en supprimant la protection de catalogue pour toutes les versions et toutes les copies d'objet sur ce support (le fichier binaire sera supprimé au cours de la prochaine maintenance quotidienne des fichiers binaires de catalogue des détails). Tous les autres enregistrements restent dans la CDB et dans la MMDB et il est possible de lancer la restauration depuis l'un de ces supports (l'exploration, par contre, est impossible).

Purge de noms de fichier

Les fichiers binaires de catalogue des détails indiquent si un fichier donné est sauvegardé sur un support associé ou non, mais les noms de fichier sont stockés dans la CDB. Un nom de fichier est considéré comme “utilisé” s’il est indiqué comme sauvegardé dans au moins un fichier binaire de catalogue des détails. Avec le temps, il se peut qu’un grand nombre de noms de fichiers soient inutilisés. Pour les supprimer, Data Protector analyse l’ensemble des fichiers binaires de catalogue des détails, puis supprime les noms de fichier non utilisés.

Purge des versions de fichier

La purge des versions de fichier représentait une tâche de maintenance importante dans OmniBack II A.03.50 et les versions précédentes. Dans Data Protector A.05.50, elle représente une tâche de maintenance quotidienne automatique mineure.

Lorsque la protection de catalogue de toutes les versions d’objet stockées sur un support spécifique expire, la maintenance quotidienne automatique des fichiers binaires DC supprime le fichier binaire correspondant.

Présentation de la gestion de la base de données IDB

Configuration de la base de données IDB

L'une des étapes les plus importantes de la configuration de votre environnement de sauvegarde Data Protector est la configuration de la base de données IDB. La configuration initiale vous permet de définir les stratégies internes concernant la taille de la base de données IDB, l'emplacement de ses répertoires, la sauvegarde de la base nécessaire si celle-ci est endommagée ou après un sinistre, ainsi que la configuration de ses rapports et notifications.

IMPORTANT

Il est fortement recommandé de planifier une sauvegarde quotidienne de la base de données IDB. La définition d'une spécification de sauvegarde pour la base de données IDB fait également partie de la configuration de cette dernière.

Maintenance de la base de données IDB

Une fois la base de données IDB configurée, sa maintenance est réduite à son minimum, en agissant principalement sur les notifications et les rapports.

Récupération de la base de données IDB

Une récupération de la base de données IDB est nécessaire si certains de ses fichiers sont manquants ou endommagés. La procédure de récupération dépend du niveau d'altération.

Reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector* pour obtenir des informations détaillées.

Croissance et performances de la base de données IDB

Pour configurer et entretenir correctement la base de données IDB, il est indispensable de bien comprendre les facteurs clés qui influent sur la croissance et les performances de la base de données IDB, ainsi que les principaux paramètres réglables que vous pouvez adapter à vos besoins. Ainsi, vous serez en mesure d'appréhender le plus efficacement possible la croissance et les performances de la base de données IDB.

Facteurs clés des performances et de la croissance de la base de données

Les facteurs clés des performances et de la croissance de la base de données IDB sont les suivants :

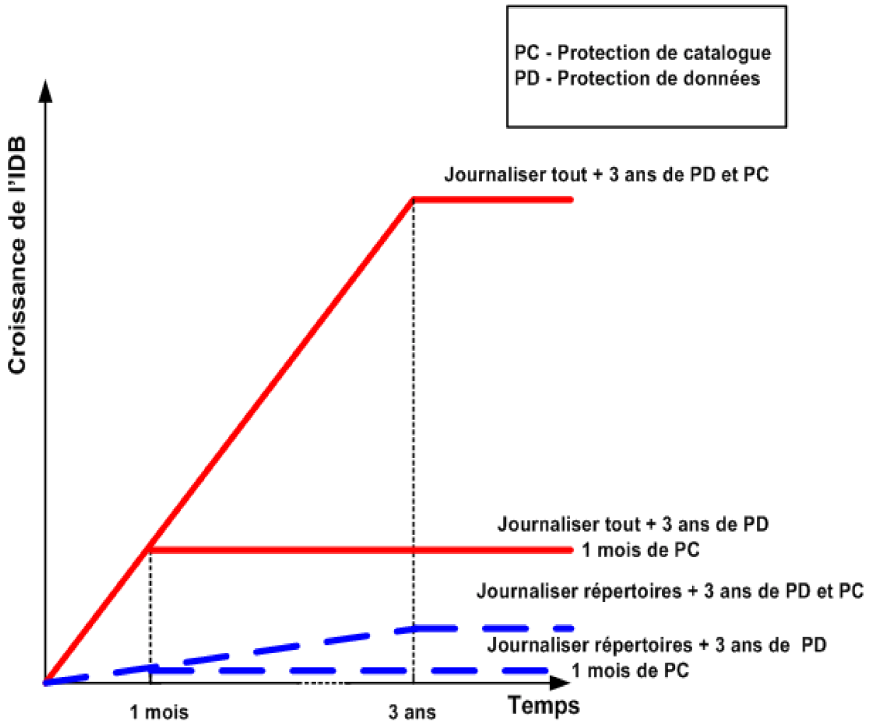
- Paramètres de niveau de journalisation :
  le niveau de journalisation indique le volume de données écrites dans l'IDB pendant la sauvegarde. Plus le niveau de journalisation utilisé est détaillé, plus l'IDB est influencée. Pour plus d'informations, reportez-vous à la section "Croissance et performances de la base de données IDB : paramètres clés réglables" à la page 217.
- Paramètre de protection de catalogue :
  la protection de catalogue détermine la durée pendant laquelle les informations sur les données sauvegardées sont disponibles dans l'IDB. Plus la période de protection de catalogue définie est longue, plus l'IDB est influencée. Pour plus d'informations, reportez-vous à la section "Croissance et performances de la base de données IDB : paramètres clés réglables" à la page 217.
- Nombre de fichiers sauvegardés :
  Data Protector garde une trace de chaque fichier et de sa version. L'incidence des différents types de sauvegarde sur la base de données IDB n'est pas la même. Pour obtenir des informations sur les différents types de sauvegarde, reportez-vous à la section "Sauvegardes complètes et incrémentales" à la page 68.
- Nombre de sauvegardes :
  plus les sauvegardes sont fréquentes, plus le volume d'informations stockées dans la base de données IDB est important.

- Variations du système de fichiers :
  le nombre de fichiers créés et supprimés entre les sauvegardes peut avoir une influence significative sur la croissance de la partie des noms de fichier de la base de données IDB. Le `rapport sur les variations du système` peut vous apporter des informations utiles. Pour éviter un accroissement de la base de données IDB dû aux variations du système de fichiers, utilisez le niveau de journalisation `Journaliser répertoires`.
- Croissance de votre environnement de sauvegarde :
  le nombre de systèmes en cours de sauvegarde dans la cellule agit sur la croissance de la base de données IDB. Il est conseillé de planifier la croissance de votre environnement de sauvegarde.
- L'encodage de caractères utilisé pour vos noms de fichier (applicable sous UNIX uniquement) :
  selon l'encodage du nom de fichier, un caractère du nom de fichier peut occuper d'un à trois octets dans la base IDB. Par exemple, les noms de fichier codés via le système Shift-JIS occupent jusqu'à trois octets dans la base IDB, alors que les noms de fichier codés en ASCII pur occupent seulement un octet. L'encodage des caractères est pertinent pour la croissance de la partie nom de fichier de la base IDB sous UNIX (sous Windows, tous les caractères occupent deux octets dans la base IDB).
- Nombre de copies d'objet et de miroirs d'objet :
  plus vous créez de copies d'objet et de miroirs d'objet, plus les informations stockées dans la base IDB sont nombreuses. Pour les copies d'objet et les miroirs d'objet, la base IDB stocke les mêmes informations que pour les objets sauvegardés, à l'exception des noms de fichier.

Croissance et performances de la base de données IDB : paramètres clés réglables

Le niveau de journalisation et la protection de catalogue sont les principaux facteurs de croissance et de performance de la base de données IDB. Leur impact sur la base de données IDB dépend des paramètres utilisés. Pour obtenir une représentation graphique de l'impact des différents paramètres concernant les niveaux de journalisation et la protection de catalogue, reportez-vous à la figure 5-2 à la page 218.

Figure 5-2 **Influence du niveau de journalisation et de la protection de catalogue sur la croissance de la base de données IDB**



Niveau de journalisation en tant que paramètre clé réglable de la base de données IDB

Qu'est-ce que le niveau de journalisation ?

Le niveau de journalisation détermine la quantité de détails figurant dans la base IDB à propos des fichiers et des répertoires sauvegardés. Vous pouvez toujours restaurer vos données, sans tenir compte du niveau de journalisation utilisé pendant la sauvegarde.

Data Protector propose quatre niveaux de journalisation permettant de contrôler la quantité de détails sur les fichiers et répertoires écrits dans l'IDB :

Tableau 5-1

Journaliser tout	Journalise toutes les informations détaillées sur les fichiers et répertoires sauvegardés (noms, versions et attributs).
Fichiers journaux	Journalise toutes les informations détaillées sur les fichiers et répertoires sauvegardés (noms et versions). Cela représente environ 30 % des informations détaillées sur les fichiers et répertoires sauvegardés.
Journaliser répertoires	Journalise toutes les informations détaillées sur les répertoires sauvegardés (noms, versions et attributs). Cela représente environ 10 % de toutes les informations détaillées sur les fichiers et répertoires sauvegardés.
Pas de journalisation	Aucune information sur les fichiers et répertoires sauvegardés n'est enregistrée dans la base de données IDB.

Les différents paramètres agissent sur la croissance de la base de données IDB, la vitesse de sauvegarde et la capacité d'exploration des données.

Impact sur les performances

Le niveau de journalisation indique le volume de données écrites dans la base de données IDB pendant une sauvegarde. Il agit également sur la vitesse de la base de données IDB et donc sur le processus de sauvegarde.

Niveau de journalisation et exploration pour la restauration

Lorsque vous changez le niveau des informations stockées, vous modifiez vos possibilités d'exploration des fichiers à l'aide de l'interface Data Protector pendant une restauration. Si l'option `Pas de journalisation` est sélectionnée, l'exploration est impossible ; si l'option `Journaliser répertoires` est sélectionnée, l'exploration des répertoires est possible ; si l'option `Journaliser fichiers` est sélectionnée, vous pouvez explorer les fichiers et les répertoires, mais les attributs de fichier (taille, dates de création et de modification, etc.) ne sont pas affichées.

Il vous est toujours possible de restaurer vos données, quel que soit le niveau de journalisation défini :

- Au lieu d'explorer vos données, vous pouvez toujours sélectionner manuellement un fichier à restaurer (si vous connaissez le nom du fichier).
- Vous pouvez également récupérer des informations sur les données sauvegardées à partir des supports.

Niveau de journalisation et vitesse de restauration

La vitesse de restauration est approximativement la même lorsque les options `Journaliser tout`, `Journaliser répertoires` ou `Journaliser fichiers` sont sélectionnées.

Si l'option `Pas de journalisation` est sélectionnée, la vitesse de restauration peut être plus lente en cas de restauration de fichiers individuels. C'est dû au fait que Data Protector doit lire toutes les données depuis le début d'un objet avant de trouver un ficher à restaurer.

Dans le cas d'une restauration complète du système, l'objet doit de toute façon être intégralement lu. Les paramètres de niveau de journalisation ne jouent donc pas un rôle très important.

Protection de catalogue en tant que paramètre clé réglable de l'IDB

Qu'est-ce que la protection de catalogue ?

La protection de catalogue détermine la durée pendant laquelle les informations sur les données sauvegardées sont disponibles dans l'IDB. Cette notion diffère de la protection de données, qui détermine la durée pendant laquelle les données sauvegardées sont disponibles sur le support lui-même. Si aucune protection de catalogue n'est définie, la restauration des données reste possible. Toutefois vous ne pourrez pas les explorer via l'interface Data Protector.

La protection de catalogue est basée sur le principe que les dernières données stockées sont les plus importantes et les plus sollicitées. Les anciens fichiers sont rarement recherchés, il est donc moins gênant que leur recherche prenne plus de temps.

Expiration de la protection de catalogue

Lorsque la protection de catalogue arrive à expiration, les informations ne sont pas immédiatement supprimées de l'IDB. Data Protector les supprime automatiquement une fois par jour. Les informations de l'IDB

étant organisées par support, la protection de catalogue doit arriver à expiration pour tous les objets du support pour que les données soient entièrement supprimées.

Impact sur les performances

Les paramètres de protection de catalogue n'ont aucun effet sur les performances de la sauvegarde.

Protection de catalogue et restauration

Lorsque la protection de catalogue arrive à expiration, les données sont restaurées comme si elles avaient été sauvegardées avec l'option `Pas de journalisation`. Reportez-vous à la section "Niveau de journalisation en tant que paramètre clé réglable de la base de données IDB" à la page 218.

Utilisation recommandée du niveau de journalisation et de la protection de catalogue

Utilisez toujours la protection de catalogue

Définissez toujours un niveau raisonnable de protection de catalogue, excepté lorsque l'option `Pas de journalisation` est sélectionnée (dans ce cas, la protection de catalogue ne s'applique pas).

Si vous définissez la protection de catalogue sur `Permanent`, les informations de l'IDB ne sont supprimées que lorsque les supports sont exportés ou supprimés. Dans ce cas, la taille de l'IDB augmente de manière linéaire jusqu'à la fin de la période de protection des données, même si le nombre de fichiers de la cellule ne change pas. Par exemple, si la période de protection des données est d'un an et que les supports sont recyclés, la croissance significative de l'IDB s'arrête au bout d'un an. L'ajout de nouveaux catalogues équivaut approximativement à la suppression des anciens. Si la protection de catalogue est définie sur quatre semaines, la croissance significative de l'IDB s'arrête au bout de quatre semaines. Dans ce cas, l'IDB est 13 fois plus volumineuse si la protection de catalogue est réglée sur `Permanent`.

Il est recommandé de définir la protection de catalogue de façon à ce qu'elle couvre au moins la dernière sauvegarde complète. Vous pouvez par exemple la définir sur 8 semaines pour les sauvegardes complètes et sur une semaine pour les sauvegardes incrémentales.

Utilisez différents niveaux de journalisation dans la même cellule

Une cellule est souvent constituée de serveurs de messagerie (ou équivalents) qui génèrent quotidiennement un grand nombre de fichiers, de serveurs de bases de données qui stockent toutes les informations dans un groupe de fichiers et de stations de travail utilisateur. Les variations de ces systèmes étant assez différentes, il est très difficile de

conseiller un réglage qui leur conviendrait à tous. Il est donc recommandé de créer plusieurs spécifications de sauvegarde avec les paramètres de niveau de journalisation suivants :

- Pour les serveurs de messagerie, choisissez l'option `Journaliser répertoires`.
- Pour les serveurs de base de données, aucune journalisation n'est nécessaire puisqu'ils possèdent leurs propres règles de restauration. Par conséquent, utilisez l'option `Pas de journalisation`.
- Pour les stations de travail, les options `Journaliser tout` ou `Journaliser fichiers` permettent la recherche et la restauration de différentes versions de fichiers. Lorsque l'option `Journaliser répertoires` ou `Pas de journalisation` est sélectionnée pour une sauvegarde, vous pouvez importer les catalogues à partir des supports, ce qui vous offre la possibilité d'explorer l'objet sélectionné en relativement peu de temps. Pour obtenir des informations sur l'importation de catalogues à partir des supports, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Niveaux de journalisation différents pour les copies d'objet

Les objets sauvegardés et les copies ou les miroirs de ces objets peuvent présenter le même niveau de journalisation ou un niveau de journalisation différent. Selon votre stratégie de sauvegarde, le niveau de journalisation sélectionné pour les copies d'objet peut être plus ou moins détaillé que celui des objets source.

Par exemple, vous pouvez spécifier l'option `Pas de journalisation` pour les miroirs d'objet si vous créez ces miroirs simplement pour garantir l'aboutissement d'une session de sauvegarde. Vous pouvez aussi choisir l'option `Pas de journalisation` pour un objet sauvegarde afin d'augmenter les performances de l'opération de sauvegarde, puis choisir l'option `Journaliser tout` pour cet objet au cours d'une session de copie d'objet ultérieure.

Particularités des petites cellules

Si le nombre de fichiers d'une cellule est peu important et n'évolue pas (un million de fichiers ou moins) et si les systèmes de la cellule réalisent les activités professionnelles habituelles, vous pouvez toujours utiliser l'option par défaut de Data Protector, `Journaliser tout`. Cependant, vous devez être attentif à la croissance de l'IDB et définir un niveau raisonnable de protection de catalogue.

Particularités des grandes cellules

Si le nombre de fichiers atteint plusieurs dizaines de millions ou que des dizaines de milliers de fichiers sont générés par jour alors que vous avez sélectionné l'option `Journaliser tout`, la vitesse de sauvegarde et la croissance de l'IDB vont rapidement devenir problématiques.
Dans une telle situation, vous avez la possibilité de :

- Réduire le niveau de journalisation au niveau le plus bas possible. Le fait de sélectionner l'option `Journaliser fichiers` peut diviser la taille de l'IDB par trois et l'option `Journaliser répertoires` environ par dix. Cela dépend bien sûr de la nature des systèmes de fichiers de la cellule.
- Réduire la protection de catalogue au minimum.
- Diviser la cellule en deux. Enfin, vous pouvez également créer une autre base de données IDB et y rediriger la moitié des systèmes.

Vous pouvez configurer le `rapport sur les variations du système` afin d'obtenir des informations sur les variations de la croissance des noms de fichier sur un client particulier.

Estimation de la taille de l'IDB

Si vous effectuez principalement des sauvegardes de systèmes de fichiers, la base de données IDB peut dans certaines conditions atteindre une taille significative (supérieure à 16 Go). Si vous réalisez des sauvegardes d'images disque ou de bases de données, l'IDB ne dépassera probablement pas 2 Go.

Méthode préconisée pour estimer la taille de l'IDB

Le moyen le plus pratique et le plus recommandé pour estimer la taille de l'IDB consiste à utiliser l'outil Internal Database Capacity Planning Tool (planification des capacités de la base de données IDB). Son emplacement est le suivant :

- Sur le système Gestionnaire de cellule UNIX : `/opt/omni/doc/C/IDB_capacity_planning.xls`
- Sur le système Gestionnaire de cellule Windows : *<répertoire_Data_Protector>*`\docs\IDB_capacity_planning.xls`

Cet outil permet également d'estimer la taille de l'IDB dans les environnements comportant des bases de données en ligne (Oracle, SAP R/3).

Autre méthode d'estimation de la taille de l'IDB

Vous pouvez également utiliser les informations suivantes pour estimer l'espace disque que l'IDB occupera après la première année de sauvegarde :

Formule de base

La taille de chaque partie clé de la base de données est calculée séparément. La formule de base est la suivante :

$$IDB = MMDB + CDB(obj + pos) + CDB(Fnames) + DCBF + SMBF$$

Notez que *CDB (obj + pos)* correspond à la taille de la CDB sans les noms de fichier.

Pour obtenir des informations sur les parties de l'IDB, reportez-vous à la section "Architecture de la base de données IDB" à la page 206.

Modèle

Pour faciliter les calculs et les rendre plus transparents, l'environnement de sauvegarde a été légèrement simplifié. L'estimation part du principe qu'il n'y a qu'une spécification de sauvegarde et que celle-ci a été créée pour sauvegarder des systèmes de fichiers.

Une fois que vous avez estimé la taille de l'IDB dans l'environnement simplifié, vous pouvez recommencer l'opération pour d'autres spécifications de sauvegarde, puis compiler vos résultats.

Paramètres d'entrée pour calculer la taille de l'IDB

Les formules utilisées dans cette section possèdent deux types d'entrée : les paramètres de l'environnement de sauvegarde et les réglages Data Protector.

Paramètres d'entrée de l'environnement de sauvegarde

L'environnement de sauvegarde est constitué des paramètres d'entrée suivants :

- *AmountOfData*
  Volume de données dans une sauvegarde complète. Pour obtenir cette information, effectuez une sauvegarde et laissez Data Protector faire le calcul.
- *NoOfFiles*
  Nombre de fichiers et de répertoires compris dans une sauvegarde complète. Pour obtenir cette information, effectuez une sauvegarde, puis configurez les `Rapports sur les sessions d'une période -> Liste des sessions de sauvegarde`.

- *NoOfFilesPerDir*
  Nombre moyen de fichiers dans un répertoire. Dans la plupart des cas, une valeur de 10 est correcte. Ne choisissez pas une valeur inférieure à 5.
- *IncrRatio*
  Pourcentage du volume de données (ou nombre de fichiers) sauvegardées au cours de sauvegardes incrémentales et complètes. Par exemple, une valeur de 0,05 signifie que 5 pour cent des fichiers sont sauvegardés dans une sauvegarde incrémentale moyenne.
- *NoOfObjects*
  Nombre d'objets (points de montage/lecteurs) sauvegardés.

Les réglages Data Protector et leurs paramètres d'entrée

Les réglages Data Protector utilisés pour les calculs comprennent notamment la protection de données, la protection de catalogue, le niveau de journalisation, la planification de sauvegardes complètes et incrémentales, la simultanéité de périphérique et la taille de segment.

Certains de ces réglages étant difficiles à utiliser dans les formules, les paramètres d'entrée auxiliaires suivants sont requis :

- *NoOfFullsDP*
  Nombre de sauvegardes complètes réalisées sur la durée de l'intervalle de protection des données. Par exemple, si une sauvegarde complète est effectuée une fois par semaine et que la durée de la protection de données a été définie sur 1 an, la valeur est de 52. Si le paramètre défini pour la protection est `Permanent`, faites le calcul en considérant qu'elle est définie sur une année.
- *NoOfIncrementalsDP*
  Nombre de sauvegardes incrémentales réalisées sur la durée de l'intervalle de protection des données.
- *NoOfFullsCP*
  Nombre de sauvegardes complètes réalisées sur la durée de l'intervalle de protection de catalogue.
- *NoOfIncrementalsCP*
  Nombre de sauvegardes incrémentales réalisées sur la durée de l'intervalle de protection de catalogue.
- *LogLevelFactor*
  La valeur de ce facteur est de 1 si le niveau de journalisation est `Journaliser tout` ou `Journaliser fichiers`, 1/*FilesPerDir* si le

niveau de journalisation est `Journaliser répertoires` et 0 si le niveau de journalisation est `Aucun`. L'estimation 1/*FilesPerDir* nécessite au moins 5 fichiers par répertoire pour être exacte.

- *DeviceConcurrency*
  Nombre d'Agents de disque écrivant simultanément sur un périphérique.
- *SegmentSize*
  Taille du segment de données utilisé. Par exemple, la taille d'un segment DLT est de 2 Go par défaut.

Taille de la MMDB

La MMDB est généralement petite et son volume augmente lentement. A moins que vous n'utilisiez des dizaines de milliers de supports, il est raisonnable de supposer que la MMDB ne dépassera pas 30 Mo.

Si le nombre de supports utilisés est élevé, la mémoire risque d'être fortement sollicitée par l'IDB et les sauvegardes risquent d'échouer. Vous pouvez calculer les capacités de mémoire utilisées sur HP-UX à l'aide de la formule suivante :

$$RDSSize = 2048KB + n \times (0{,}7KB \times m + 1{,}5KB \times a)$$

où n correspond au nombre minimum de sessions simultanées ou au nombre de threads RPC (défini au niveau du fichier `velocis.ini`, la valeur par défaut étant de 3), m au nombre de supports dans le pool sélectionné et a au nombre de supports dans l'IDB.

Les tailles moyennes sont les suivantes :

- *0,7 KB* correspond à la taille d'un enregistrement moyen dans l'IDB (par pool).
- *1,5 KB* correspond à la taille d'un enregistrement moyen dans un fichier binaire (tout support).
- *2048 KB* correspond à la taille RDS initiale.

La formule ci-dessus peut être utilisée pour obtenir une estimation globale de la quantité de mémoire utilisée par le processus serveur de base de données Raima (RDS). Toutefois, le résultat ne permet pas de déterminer la quantité de mémoire maximale du RDS : en effet, sur HP-UX, la mémoire n'est pas renvoyée au système une fois libérée. S'il est nécessaire d'allouer des fragments importants de mémoire, le système de gestion de mémoire ne fragmente pas la mémoire et renvoie

généralement plusieurs fragments importants en un seul bloc. Dans ces conditions, les petits fragments de mémoire restent disponibles mais ne sont pas utilisés, ce qui entraîne une augmentation de la quantité de mémoire utilisée. Lorsque la quantité de mémoire utilisée atteint la limite maximale autorisée (930 Mo), la réallocation échoue.

Dans l'exemple ci-dessous, le calcul de la mémoire utilisée s'appuie sur 50 % de la taille maximale autorisée (465 Mo). On suppose que tous les supports se trouvent dans le même pool.

$$
\begin{aligned}
&465MB = 2048KB + 3 \times (0{,}7KB \times m + 1{,}5KB \times a),\ a = m\\
&465MB = 2048KB + 3 \times (0{,}7KB \times m + 1{,}5KB \times m)\\
&465MB = 2048KB + 3 \times 0{,}7KB \times m + 3 \times 1{,}5KB \times m\\
&465MB - 2048KB = m \times (3 \times 0{,}7KB + 3 \times 1{,}5KB)\\
&465MB - 2048KB = m \times (2{,}1KB + 4{,}5KB)\\
&465MB - 2048KB = m \times 6{,}6KB\\
&m = (465MB - 2048KB)/(6{,}6KB)\\
&m = 71835media
\end{aligned}
$$

Taille de la CDB (objets et positions)

Formule

Sans les noms de fichier, la CDB est petite et n'augmente pas très vite. La formule permettant de calculer sa taille est la suivante :

$$CDB(obj + pos) = BASE + (NoOfMpos \times MPOS) + [NoOfObjVer \times OBJVER]$$

BASE est une constante de taille. Elle ne peut dépasser 20 Mo.

NoOfMpos correspond au nombre d'enregistrements d'emplacement de support. Il existe un enregistrement d'emplacement de support par segment écrit sur un support.

$$NoOfMpos = \frac{NoOfBackupsDP \times AmountOfData}{SegmentSize} \times DeviceConcurrency$$

MPOS et *OBJVER* sont des constantes de taille. La valeur de *MPOS* est de 124 octets. Celle de *OBJVER* est de 384 octets.

NoOfObjVer correspond au nombre de versions d'objet sauvegardées et copiées. On le calcule comme suit :

$$NoOfObjVer = NoOfObj \times (NoOfFullsDP + NoOfIncrementalsDP)$$

NoOfObj correspond au nombre d'objets figurant dans la spécification de sauvegarde ainsi qu'au nombre de copies/miroirs basés sur ces objets.

NoOfFullsDP correspond au nombre de sauvegardes complètes réalisées sur la durée de l'intervalle de protection des données.

NoOfIncrementalsDP correspond au nombre de sauvegardes incrémentales réalisées sur la durée de l'intervalle de protection des données.

Taille de la CDB (noms de fichier)

Formule

La formule permettant de calculer le nombre de noms de fichier dans l'IDB est la suivante :

$$CDB(Fnames) = NoOfFiles \times FNAME \times LogLevelFactor \times CumulativeGrowthFactor$$

FNAME est une constante représentant la taille moyenne d'un enregistrement de nom de fichier. La valeur de *FNAME* est de 75 octets.

Lors de l'estimation de la taille des noms de fichier de l'IDB, la difficulté réside dans l'estimation des variations du système de fichiers, en d'autres termes, dans l'estimation du nombre de fichiers supprimés et créés entre les sauvegardes. Ce nombre est difficile à prévoir alors que son impact est très important. Le *CumulativeGrowthFactor* (facteur de croissance cumulative) est donc utilisé pour décrire le taux entre le nombre courant de fichiers et le nombre de noms de fichier stockés dans l'IDB au bout d'un an. Par exemple, la valeur 1 signifie qu'aucun fichier n'a été créé en une année ; la valeur 10 signifie que pour chaque fichier, 9 fichiers supplémentaires ont été créés. En moyenne, cette valeur oscille entre 1,5 (valeur optimale) et 4.

Exemple

Supposons que le nombre de fichiers soit égal à 10 millions et que le niveau de journalisation soit réglé sur `Journaliser tout` (le *facteur du niveau de journalisation* est de 1). Le *facteur de croissance cumulative (Cumulative GrowthFactr)* est de 2, et la valeur *FNAME* de 75 octets. Dans un tel cas, la taille de la partie des noms de fichier est estimée à 1 Go environ.

Taille des DCBF

Formule

La formule permettant de calculer la taille des DCBF est la suivante :

$$DCBF = NoOfFiles \times NoOfBackupsCP \times FVER \times LogLevelFactor$$

NoOfBackupsCP correspond au nombre de sessions de sauvegarde réalisées dans l'intervalle de protection de catalogue. Il est calculé de la façon suivante :

$$NoOfBackupsCP = NoOfFullsCP + (NoOfIncrementalsCP \times IncrRatio)$$

FVER est défini sur 10 octets pour le niveau de journalisation `Journaliser fichiers` et à 30 octets pour le niveau de journalisation `Journaliser tout` ou `Journaliser répertoires`.

Taille des SMBF

Un SMBF est petit, augmente lentement et n'a pas de grande incidence sur la taille et la croissance de l'IDB. Vous pouvez estimer sa taille en supposant qu'un objet sauvegarde et que chaque objet miroir dans une spécification de sauvegarde et une copie d'objet dans une spécification de copie d'objet occupe 10 à 100 Ko dans la base SMBF.

6 Gestion des services

Description du chapitre

Grâce à la gestion des services, à la génération de rapports et à la surveillance, les administrateurs sont en mesure de gérer plus efficacement leurs environnements de sauvegarde. Ce chapitre décrit les concepts de base de la gestion des services et présente ses avantages tant pour la configuration autonome de Data Protector que pour son intégration avec les produits de gestion de services HP OpenView.

Il s'organise comme suit :

"Présentation" à la page 233

"Fonctionnalité Data Protector native" à la page 236

"Intégrations pour la gestion des services" à la page 246

Présentation

Les services informatiques des entreprises font de plus en plus appel aux outils, techniques et méthodes de gestion des services pour fixer leurs objectifs en termes de niveau de service, évaluer leurs prestations par rapport à ces objectifs et justifier leur expansion future.

Les groupes informatiques devant gérer le risque de perte de données, la sauvegarde et la récupération de données sont des éléments essentiels dans la prestation et la gestion des services informatiques. Erreur des utilisateurs, virus, accès non autorisé aux données, défaillance occasionnelle du périphérique de stockage : autant d'éléments qui menacent en permanence les données. Or, une perte de données stratégiques peut coûter à l'entreprise des milliers, voire des millions de dollars pour chaque heure d'indisponibilité.

Les utilisateurs, en revanche, considèrent parfois la sauvegarde des données comme une opération qui, pendant son exécution, peut ralentir ou empêcher leur accès à certains services. Néanmoins, sans cette activité essentielle, la disponibilité permanente et en temps voulu des services peut être nettement compromise.

Si toutes les données sont menacées, toutes n'ont pas les mêmes exigences en termes de capacité de récupération. Ainsi, les départements informatiques doivent assurer pour les données stratégiques un niveau de protection supérieur à celui des données moins essentielles, et ce à un coût réduit.

Les évaluations et les rapports de gestion des services comptent parmi les principaux outils que les responsables des services informatiques peuvent utiliser pour démontrer la valeur fournie à l'entreprise ainsi que pour conserver des structures de coûts compétitives. Les fournisseurs de services utilisent des contrats de niveau de service (SLA) afin de définir les objectifs de disponibilité et de performances et de fixer ainsi les attentes des parties.

Une surveillance permanente et la génération périodique de rapports sont nécessaires pour savoir si les dispositions du SLA sont respectées. Data Protector offre en standard des outils de surveillance, de notification et de génération de rapports permettant de documenter les opérations de sauvegarde et de récupération. L'intégration avec d'autres produits de gestion de services OpenView permet de regrouper sur une

seule console les vues, données de performance et autres fonctionnalités, vous donnant ainsi un meilleur aperçu de la prestation globale de services informatiques.

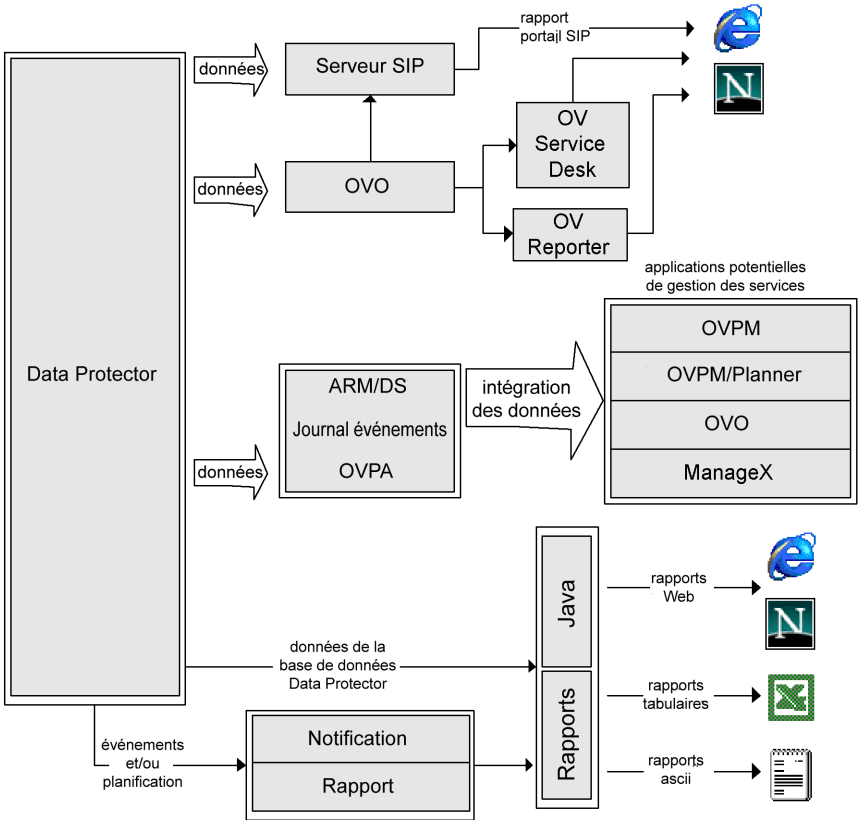
Data Protector fournit aux responsables des services informatiques des données essentielles pour la surveillance et la planification fonctionnelles des opérations de sauvegarde et de récupération des données. Ces données peuvent être utilisées dans les activités consistant à planifier la disponibilité du service et la récupération, lesquelles sont fondamentales en cas de signature d'accords de service. De plus, les informations fournies par Data Protector peuvent être utilisées pour mettre en place des modèles de gestion des coûts et de facturation interne afin de permettre une véritable gestion financière du service informatique.

Data Protector et la gestion des services

Data Protector offre des fonctions de gestion des services et peut être associé à des applications de gestion des services, telles que ManageX, OpenView Performance Agent (anciennement MeasureWare Agent), OpenView Reporter, OpenView Service Desk et OpenView Service Information Portal.

Dans Data Protector, on distingue deux catégories de gestion des services : native et résultant de l'intégration d'autres applications. Les éléments de chaque catégorie sont détaillés plus loin dans ce chapitre.

Figure 6-1 Flux des données de la gestion des services



Fonctionnalité Data Protector native

La fonctionnalité décrite dans les sections suivantes est fournie en standard avec Data Protector.

Fonctions clé

- Data Protector a été conçu pour assurer le suivi du temps écoulé pour les opérations clé et pour enregistrer ces données ainsi que le volume des données à l'aide de l'API Application Response Measurement version 2.0 (API ARM 2.0). L'enregistrement de ces données peut être effectué à l'aide de HP OpenView Performance Agent (OVPA).
- Le contrôle intégré des sessions en cours permet de réagir instantanément aux événements survenant dans votre environnement de sauvegarde.
- Le moteur de notification et de génération de rapports intégré de Data Protector permet de recevoir des rapports concis ainsi que des avertissements immédiats sous différents formats (ASCII, HTML et formats compatibles tableurs) et selon différentes méthodes : e-mail, SNMP, diffusion (disponible uniquement sous Windows), enregistrement dans un fichier et envoi vers une commande externe. Le moteur de notification intégré de Data Protector étant en mesure d'envoyer des avertissements via SNMP, il est possible d'intégrer quasiment toutes les applications capables de recevoir des interruptions SNMP.
- L'intégration de Data Protector avec HP OpenView Operations permet de recevoir des avertissements de Data Protector sur la console OVO et d'effectuer des actions automatiques.
- La capacité de Data Protector d'envoyer les événements majeurs et critiques au journal d'événements Windows ouvre la voie à toute une série de possibilités d'intégration très utiles.
- L'intégration avec HP OpenView ManageX transfère automatiquement les événements majeurs et critiques de Data Protector vers la console ManageX. Vous pouvez paramétrer des actions automatiques destinées à réagir aux pannes dans l'environnement de sauvegarde.
- Grâce à sa fonction intégrée de génération de rapports Java en ligne, Data Protector vous permet de créer des rapports en ligne depuis n'importe quel endroit du réseau (même à distance) sans que

l'interface utilisateur Data Protector ne soit nécessairement installée sur votre ordinateur local. Vous devez disposer pour cela d'un navigateur Web.

Application Response Measurement version 2.0 (API ARM 2.0)

Qu'est-ce que l'ARM ?

L'API ARM est une norme de plus en plus utilisée pour la mesure du temps de réponse de bout en bout des transactions dans les environnements distribués. Les applications qui utilisent l'API ARM se comportent comme des sources d'informations de temps de réponse (et aussi d'informations fournies par l'utilisateur pouvant être pertinentes pour une transaction particulière) pour les outils de contrôle et de gestion de systèmes compatibles ARM, tels que HP OpenView Performance Agent (OVPA). OVPA enregistre les informations de transaction ARM dans son référentiel pour l'analyse et la génération de rapports ultérieures. Il peut également produire des avertissements en temps réel (ou "alarmes") lorsque le temps écoulé pour une transaction donnée, telle qu'une opération de sauvegarde, dépasse une limite prédéfinie. Lorsqu'un avertissement en temps réel est émis, un certain nombre d'actions sont possibles, parmi lesquelles : informer une console d'opérations centrale, telle que HP OpenView Operations, appeler un opérateur système sur son récepteur de poche, déclencher une action automatisée pour résoudre le problème.

Tableau 6-1 Fonctionnalité ARM

Description de la transaction (ARM 1,0)	Données supplémentaires envoyées vers ARM (ARM 2.0)	Utilisation
Durée de la session de spécification de sauvegarde	Données traitées [Mo]	Planification de la disponibilité et de la récupération. Facturation interne.

Tableau 6-1 Fonctionnalité ARM

Description de la transaction (ARM 1,0)	Données supplémentaires envoyées vers ARM (ARM 2.0)	Utilisation
Durée de la session de sauvegarde d'un objet	Données traitées [Mo]	Planification de la disponibilité et de la récupération. Facturation interne.
Durée de la session de restauration	Données récupérées [Mo]	Planification de la disponibilité et de la récupération
Durée de la vérification de la base de données IDB	Taille de la base de données IDB [Mo]	Gestion de l'architecture Data Protector
Durée de la purge de la base de données IDB	Volume de la base de données IDB après la purge et nombre d'enregistrements purgés	Gestion de l'architecture Data Protector

Data Protector étant déjà doté de l'ARM, il est relativement facile de l'associer à une application comme OVPA prenant en charge l'API ARM. Sur les plates-formes Windows, cela se fait de manière entièrement automatique. Lorsque Data Protector est installé sur un système où OVPA se trouve déjà (ou vice versa), les données de transaction apparaissent immédiatement dans OVPA et HP OpenView Performance Manager (OVPM). Sous HP-UX, vous devez uniquement créer un lien d'une bibliothèque OVPA vers un répertoire Data Protector. Pour plus d'informations, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Une autre interface possible entre OVPA et Data Protector est l'Intégration des sources de données (DSI). Cette possibilité est importante si l'application que vous utilisez pour le suivi des transactions n'est pas compatible ARM 2.0. ARM 1.0 ne permet d'enregistrer que des données relatives au temps, telles que la durée d'une session de sauvegarde. Avec la DSI, il devient possible

d'enregistrer toute donnée pouvant être extraite de la ligne de commande vers des outils tels que OPVA. Vous pouvez ainsi personnaliser considérablement les rapports.

Intégration avec HP OpenView Operations

Fonctionnalité de l'intégration de OVO avec Data Protector

Data Protector s'intègre avec HP OpenView Operations (OVO). OVO simplifie la gestion des grands environnements en permettant à l'opérateur de contrôler et d'administrer le réseau et les applications à partir d'un seul point. Une fois que Data Protector est intégré à l'environnement OVO, l'administrateur réseau peut immédiatement voir si une erreur survient lors de la sauvegarde et réagir en fonction des informations données. Les messages Data Protector peuvent s'afficher dans la fenêtre OVO prévue à cet effet.

Intégration avec ManageX

Fonctionnalité de l'intégration de ManageX avec Data Protector

L'intégration de ManageX avec Data Protector peut uniquement s'effectuer sur les plates-formes Windows. Elle offre les fonctionnalités suivantes :

- Data Protector enregistre dans le journal d'événements de Windows tous les messages majeurs et critiques apparaissant lors d'une sauvegarde, d'une restauration ou de toute autre opération. ManageX utilise ensuite ces événements et les transfère vers la console ManageX, pour qu'un opérateur puisse agir en conséquence.
- Contrôle des services

  ManageX contrôle tous les services Data Protector s'exécutant sur le Gestionnaire de cellule ainsi que tout système client Data Protector. En cas de dysfonctionnement de l'un des ces services, ManageX en avertit immédiatement l'opérateur. ManageX peut également être configuré pour essayer automatiquement de relancer le service défectueux.

Ces fonctionnalités sont déjà intégrées dans ManageX 3.5 et ses versions supérieures. Pour utiliser cette intégration, il suffit de distribuer ces fonctionnalités ManageX sur les systèmes Data Protector.

Interruptions SNMP

Les interruptions SNMP permettent à une application de gestion des services de recevoir et de traiter un message d'interruption SNMP lorsqu'un événement Data Protector se produit ou lorsqu'une interruption SNMP est envoyée suite au déclenchement d'un mécanisme de vérification et de maintenance Data Protector. Pour plus d'informations sur le mécanisme de vérification et de maintenance Data Protector et sur la configuration des interruptions SNMP, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Le moniteur

Elément de l'interface utilisateur de Data Protector, le moniteur Data Protector permet de superviser les sessions de sauvegarde, de restauration et de gestion des supports en cours et d'en corriger les erreurs.

Via le moniteur, vous pouvez surveiller toutes les sessions d'une cellule et visualiser les messages détaillés ainsi que l'état actuel de ces sessions. Dans un environnement multicellules, vous pouvez afficher les sessions qui fonctionnent sur des systèmes informatiques installés dans d'autres cellules. Depuis l'interface utilisateur du moniteur, vous pouvez abandonner une session de sauvegarde, de restauration ou de gestion des supports ou encore répondre à des demandes de "montage".

Si vous utilisez le Manager-of-Managers, vous pouvez contrôler les sessions de plusieurs cellules simultanément à partir d'une seule interface utilisateur.

Génération de rapports et notification

Data Protector a toujours intégré un large éventail de rapports exploités par les administrateurs pour gérer les systèmes Gestionnaire de cellule. Désormais, les fournisseurs de services informatiques peuvent utiliser ces mêmes rapports pour indiquer si les dispositions du SLA concernant la sécurité des données sont respectées. Parmi les rapports intégrés spécifiquement dédiés à la gestion du niveau de service, citons :

- Rapports d'inventaire/d'état, comme le rapport host_not_conf, qui contient des informations sur les systèmes non protégés, le rapport dl_sched, qui répertorie toutes les sauvegardes planifiées, et le rapport media_list, qui fait l'inventaire des supports.

- Rapports d'utilisation des capacités, comme le rapport sur la licence, qui décrit l'utilisation de la licence Data Protector, et le rapport dev_unused, qui répertorie les périphériques non utilisés pour une sauvegarde (disponibles).
- Rapports de problèmes, comme le rapport backup_statistics, qui contient des informations sur les échecs de sauvegarde. L'administrateur peut recevoir une fois par heure, par jour ou par semaine un e-mail décrivant les tâches qui ont échoué et les raisons de leur échec.

Les fonctions de notification et de génération de rapports qui ont toujours fait partie intégrante du Gestionnaire de cellule (et qui ont été largement étendues depuis les versions antérieures) vous permettent également d'exécuter les opérations suivantes :

- Choisir parmi une trentaine de rapports prédéfinis (notamment les rapports sur les sessions dans une période donnée, les rapports sur la base de données IDB et les rapports d'utilisation des périphériques).
- Spécifier vos propres paramètres pour ces rapports (comme les périodes, les spécifications de sauvegarde et les groupes de sauvegardes).
- Faire un choix parmi les divers formats de sortie (tels que ASCII, HTML et formats compatibles tableurs).
- Planifier ces rapports avec le planificateur Data Protector intégré.
- Déclencher l'envoi des rapports en fonction d'événements donnés (dysfonctionnement d'un périphérique, demandes de montage ou fin de sessions, par exemple).
- Choisir parmi différents modes d'envoi la façon dont ces rapports doivent vous parvenir : e-mail, SNMP, diffusion (disponible uniquement sous Windows), enregistrement dans un fichier et envoi vers une commande externe.

Vous pouvez combiner la plupart de ces différents paramètres : formats, modes de réception, planifications et déclenchements.

En voici quelques exemples :

Exemples de rapports et de notifications

- Tous les matins, à 7:00, un rapport est créé sur toutes les sessions de sauvegarde effectuées au cours des dernières 24 heures, puis envoyé au format ASCII par e-mail à la boîte aux lettres de l'administrateur.

De plus, ce même rapport est enregistré sur votre serveur Web dans un fichier au format HTML, de sorte que d'autres utilisateurs peuvent avoir accès à ces informations.

- Dans le cas d'une défaillance d'un périphérique ou d'une demande de montage, un message de diffusion est immédiatement envoyé à la station de travail Windows de l'administrateur et une commande externe est déclenchée pour avertir l'administrateur sur son récepteur de poche.
- A la fin d'une session de sauvegarde, chaque utilisateur final dont le système a été sauvegardé reçoit un e-mail au format ASCII, dans lequel figure le rapport d'état de sauvegarde.

Journalisation et notification des événements

Le journal d'événements Data Protector est un référentiel central contenant l'ensemble des notifications ayant trait à Data Protector. Le moteur de notification intégré de Data Protector envoie des avertissements ou active le mécanisme de génération de rapports de Data Protector en fonction des entrées du journal. Le journal d'événements constitue la principale source d'informations pour les rapports de conformité au SLA dans Data Protector ou dans les applications de gestion OpenView. Les entrées du journal contribuent non seulement à la génération de rapports, mais aussi à l'envoi d'informations aux applications de gestion OpenView via le SPI Data Protector (smart plug-in), permettant ainsi à celles-ci de déclencher des actions préventives ou correctives (pour plus de détails, voir l'exemple sous 3.1).

Le moteur de notification intégré de Data Protector étant en mesure d'envoyer des avertissements via SNMP, il est possible d'intégrer avec Data Protector quasiment toutes les applications capables de recevoir des interruptions SNMP. L'intégration avec HP OpenView Operations et OpenView Reporter est un exemple d'une mise en oeuvre fondée sur les interruptions SNMP.

Le journal d'événements n'est accessible qu'aux utilisateurs Data Protector appartenant au groupe `Admin` et à ceux qui disposent des droits d'utilisateur portant sur les `rapports, les notifications et le journal d'événements`. Vous pouvez afficher ou supprimer l'ensemble des événements du journal.

Fichiers journaux Data Protector

Certaines applications de gestion des services, telles que HP OpenView Operations, vous permettent de spécifier les fichiers journaux à contrôler pour une entrée de journal spécifique et le moment où ce contrôle doit être effectué. Si l'entrée spécifiée est détectée dans le fichier, une action peut être définie. Dans OVO, cette opération est appelée *Encapsulation du fichier journal*.

Vous pouvez configurer ce type d'application de gestion des services afin de contrôler les fichiers journaux Data Protector pour des entrées de journal spécifiques (événements Data Protector) et définir une action à effectuer dans le cas où un événement Data Protector particulier est détecté.

Pour plus d'informations sur les fichiers journaux Data Protector, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*. Notez qu'aucune spécification de formatage des fichiers journaux n'est fournie.

Journal de l'application Windows

Certaines applications de gestion des services, telles que Manage X, contrôlent le journal de l'application Windows.

Pour activer le transfert automatique de tous les messages Data Protector et des messages concernant les services Data Protector (s'ils sont arrêtés) vers le journal de l'application Windows, réglez la variable `EventLogMessages` dans le fichier d'options globales Data Protector sur `1`. Pour plus d'informations sur le fichier d'options globales Data Protector, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Rapports Java en ligne

Data Protector offre une fonction de création de rapports Java en ligne permettant de configurer, d'exécuter et d'imprimer tous les rapports intégrés de Data Protector, en temps réel et de façon interactive. Pendant la génération de rapports Java, la fonctionnalité Data Protector correspondante accède directement au Gestionnaire de cellule pour extraire les données en cours. Vous pouvez mettre à disposition cet applet Java via un serveur Web, le copier sur la machine client pour un accès direct ou l'utiliser en local.

Pour utiliser cette fonction, seul un navigateur Web pris en charge est nécessaire. L'installation de l'interface Data Protector sur le système n'est pas nécessaire.

Vous pouvez utiliser la fonction de génération de rapports Java non seulement pour accéder directement à vos rapports en ligne, mais aussi pour en reconfigurer la structure (ajouter de nouveaux rapports à un programme ou modifier les paramètres d'un rapport, par exemple).

Mécanisme de vérification et de maintenance Data Protector

Data Protector offre un puissant mécanisme d'auto-vérification et de maintenance, lequel intervient quotidiennement pour améliorer la fiabilité et la prévisibilité opérationnelles du système. Les tâches d'auto-vérification et de maintenance de Data Protector comprennent les suivantes :

- Vérification "Supports libres insuffisants"
- Vérification "Expiration de la licence Data Protector"

Pour obtenir une liste complète, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Gestion centralisée, environnement distribué

Grâce au MoM Data Protector, les administrateurs peuvent gérer de façon centralisée un environnement d'entreprise composé de plusieurs systèmes Gestionnaire de cellule Data Protector. L'administrateur du système MoM effectue depuis une seule console toutes les tâches de configuration, de gestion des supports, de surveillance et d'élaboration de rapports d'état pour l'ensemble de l'entreprise. Ainsi, la gestion de nombreux systèmes Gestionnaire de cellule Data Protector s'avère tout aussi simple que celle d'un système unique. Les fournisseurs de services informatiques peuvent gérer les grands environnements de leurs clients sans avoir à embaucher de personnel supplémentaire. Pour plus d'informations sur le MoM, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Utilisation des données fournies par Data Protector

Voici quelques exemples illustrant ce qu'il est possible de faire avec les données fournies par Data Protector :

Que peut-on faire avec les données ?

- Avertissement en temps réel lorsque des sessions de sauvegarde ou de restauration dépassent le délai spécifié (OVPA).
- Création de graphiques illustrant la durée de sauvegarde des systèmes clés de votre environnement afin de déterminer la tendance générale des temps d'opération (OVPM).
- Prévisions sur la croissance de la base de données IDB, afin de pouvoir déterminer à quels moments certaines limites seront atteintes (planificateur OVPM).
- Envoi régulier de rapports par e-mail aux opérateurs de sauvegarde, aux utilisateurs finaux et aux responsables de l'entreprise (fonction de génération de rapports intégrée de Data Protector permettant l'envoi d'e-mail).
- Rapports de sauvegarde créés sur un serveur Web pour les rendre accessibles sur demande (fonction de génération de rapports intégrée de Data Protector permettant l'enregistrement au format HTML).
- Envoi d'événements Data Protector majeurs et critiques vers votre solution d'administration réseau, telle que HP OpenView Network Node Manager (moteur de notification Data Protector intégré permettant l'envoi d'interruptions SNMP).

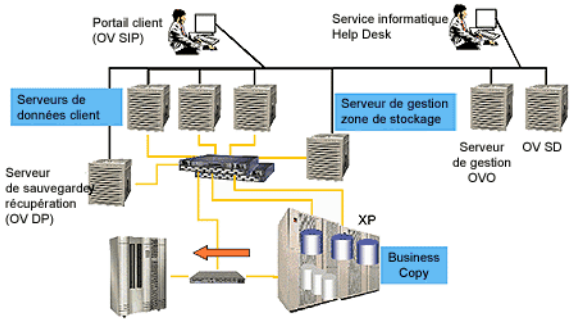
Intégrations pour la gestion des services

Les intégrations suivantes de Data Protector peuvent être installées pour simplifier la gestion des services et vous donner un accès centralisé à de puissantes fonctions de gestion des services.

Fonctions clé

- Formats de rapport standard et personnalisés.
- Interface de “dossiers d’incidents” pour Data Protector.
- Niveau de service spécifique, cohérent et mesurable.
- Informations Data Protector disponibles sur une interface Web.
- Représentation graphique des données.

Figure 6-2 **Exemple d’un environnement de fournisseur de services informatiques offrant un accès à la gestion des services via le portail client.**



Intégration Data Protector-OVO-OVR

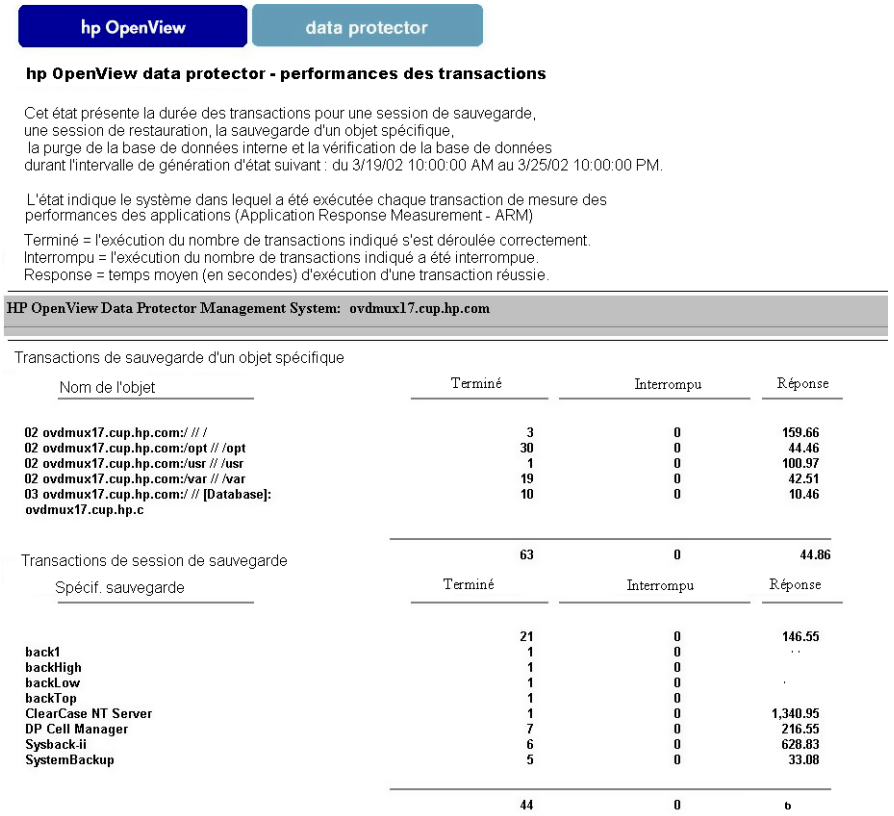
L’intégration de Data Protector avec HP OpenView Operations (OVO) est étendue grâce à l’ajout de HP OpenView Reporter 3.0 (version anglaise). A l’aide de Reporter, les fournisseurs de services peuvent générer des rapports depuis la console OVO, qui joue alors le rôle de point de gestion central. L’intégration avec Reporter ajoute une variété de nouveaux rapports dans les catégories suivantes :

- Rapports sur les sessions de sauvegarde.
- Rapports d’administration.

- Rapports sur les pools de supports.
- Performances.

Les fournisseurs de services informatiques peuvent utiliser ces rapports pour prouver à un client qu'il respecte le SLA. Par exemple, le rapport intitulé "Performances des transactions Data Protector" présente des données sur les performances du service (l'un des paramètres du SLA informatique) :

Figure 6-3 Data ProtectorExemple - OVR Data Protector



hp OpenView | data protector

hp OpenView data protector - performances des transactions

Cet état présente la durée des transactions pour une session de sauvegarde, une session de restauration, la sauvegarde d'un objet spécifique, la purge de la base de données interne et la vérification de la base de données durant l'intervalle de génération d'état suivant : du 3/19/02 10:00:00 AM au 3/25/02 10:00:00 PM.

L'état indique le système dans lequel a été exécutée chaque transaction de mesure des performances des applications (Application Response Measurement - ARM)

Terminé = l'exécution du nombre de transactions indiqué s'est déroulée correctement.
Interrompu = l'exécution du nombre de transactions indiqué a été interrompue.
Response = temps moyen (en secondes) d'exécution d'une transaction réussie.

HP OpenView Data Protector Management System: ovdmux17.cup.hp.com

Transactions de sauvegarde d'un objet spécifique

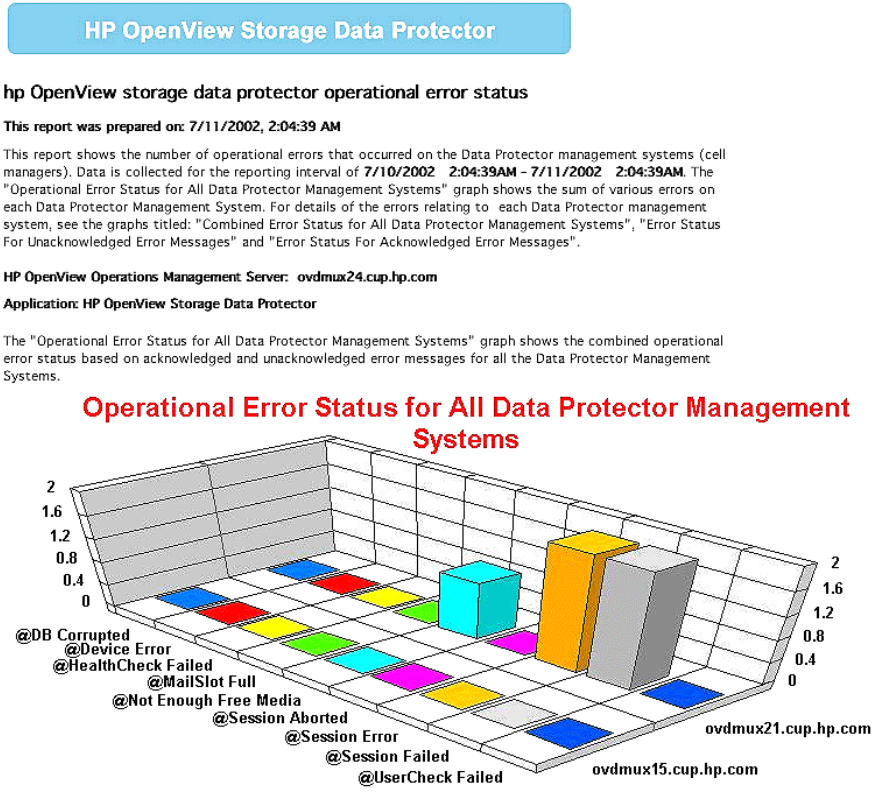
Nom de l'objet	Terminé	Interrompu	Réponse
02 ovdmux17.cup.hp.com:/ // /	3	0	159.66
02 ovdmux17.cup.hp.com:/opt // /opt	30	0	44.46
02 ovdmux17.cup.hp.com:/usr // /usr	1	0	100.97
02 ovdmux17.cup.hp.com:/var // /var	19	0	42.51
03 ovdmux17.cup.hp.com:/ // [Database]: ovdmux17.cup.hp.c	10	0	10.46
	63	0	44.86

Transactions de session de sauvegarde

Spécif. sauvegarde	Terminé	Interrompu	Réponse
	21	0	146.55
back1	1	0	
backHigh	1	0	
backLow	1	0	
backTop	1	0	
ClearCase NT Server	1	0	1,340.95
DP Cell Manager	7	0	216.55
Sysback-ii	6	0	628.83
SystemBackup	5	0	33.08
	44	0	6

Outre les rapports de conformité au SLA, un fournisseur de services informatiques peut générer des rapports opérationnels mensuels pour l'environnement Data Protector. Par exemple, le "Rapport sur l'état des erreurs de fonctionnement de Data Protector" regroupe les problèmes et peut être utilisé par le fournisseur de services informatiques à des fins de planification opérationnelle.

Figure 6-4 Rapport sur l'état des erreurs de fonctionnement

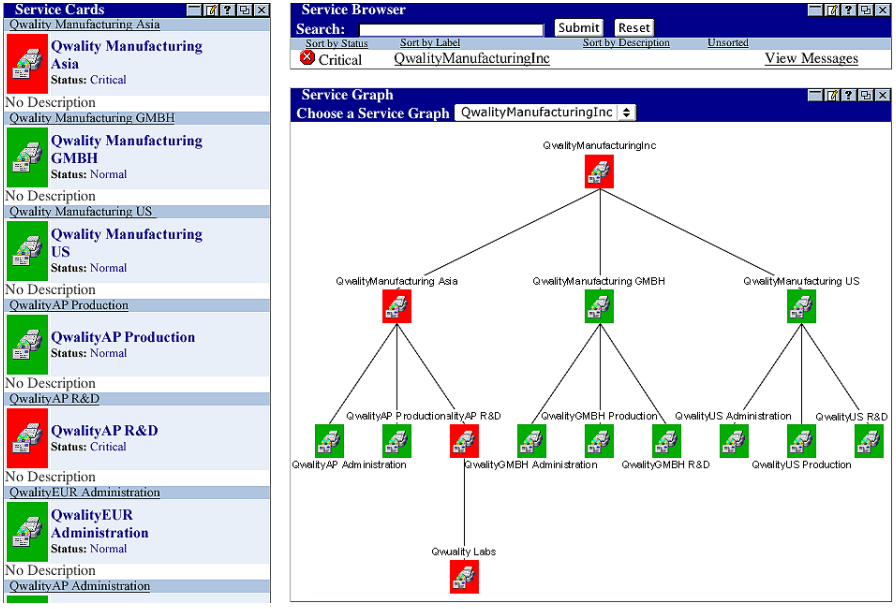


Data Protector-OVO-SIP

SIP peut vous offrir un aperçu des services que vous fournissez. Au lieu de vous donner une vue généralisée de votre infrastructure, SIP personnalise les informations associées à chacun de vos clients et affiche des données spécifiques à leurs environnements.

Grâce à cette intégration, vous pouvez offrir à vos clients un aperçu du niveau des opérations de protection de données qu'ils externalisent. Cette intégration utilise des composants OVO pour représenter graphiquement le réseau de stockage.

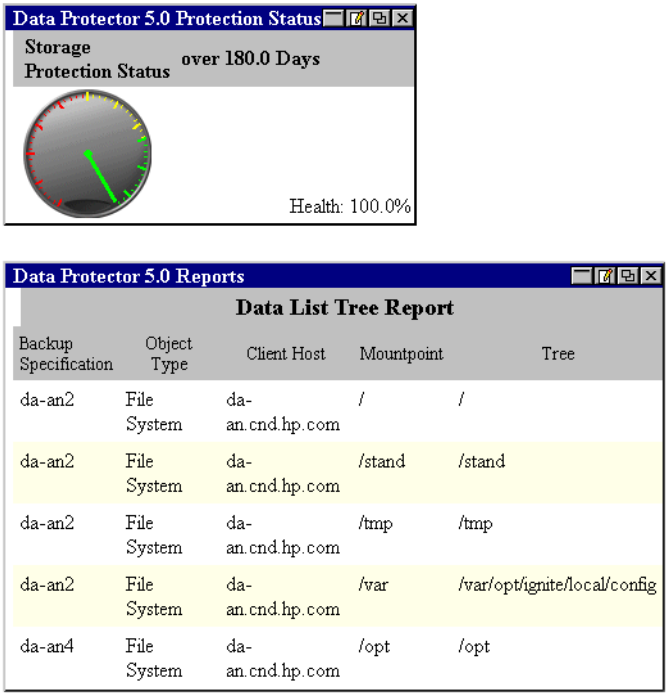
Figure 6-5 Exemple - OVO-SIP Data Protector



Data Protector-SIP

Cette intégration fait également appel à SIP pour fournir des informations Data Protector via une interface Web. OVO ne doit pas nécessairement être installé. Cette intégration présente les données sous forme de tables et de jauges.

Figure 6-6 Exemple d'une intégration directe de SIP



Intégration de Data Protector avec HP OpenView Service Desk

Service Desk est une solution destinée aux services d'assistance. Elle permet aux entreprises d'assistance technique de traiter en un seul flux de travail les processus de configuration, d'assistance, de résolution d'incidents, de résolution de problèmes et de gestion des changements. Service Desk automatise et régule les processus de dépannage informatique. Il stocke les SLA et s'assure que les services d'assistance sont bien conformes à ces derniers.

Lorsqu'il est intégré à Data Protector, Service Desk surveille (sans intervention humaine) le temps nécessaire à la résolution des problèmes liés aux sauvegardes, tels que l'ajout de supports ou le redémarrage d'une sauvegarde ayant échoué, améliorant ainsi les fonctions de surveillance et de mesure de Data Protector.

Service Desk gère le flux de travail du service d'assistance, mesure le niveau de qualité des services et génère des rapports établissant la conformité avec le SLA. L'intégration de Data Protector A.05.50 et de Service Desk permet au personnel d'assistance d'accéder aux données de Data Protector et de parvenir à la résolution des problèmes opérationnels en temps voulu, avant que ceux-ci n'affectent les services vitaux de protection des données.

7 Fonctionnement de Data Protector

Description du chapitre

Ce chapitre décrit le fonctionnement de Data Protector. Il explique les processus (sous UNIX) et les services (sous Windows) Data Protector, ainsi que les sessions de sauvegarde, de restauration et de gestion des supports.

Il s'organise comme suit :

Processus ou services Data Protector

Data Protector exécute en arrière-plan différents processus (sous UNIX) et services (sous Windows) qui lui permettent de lancer les sessions de sauvegarde et de restauration. Il fournit les voies de communication nécessaires, active les sessions de sauvegarde et de restauration, lance les Agents de disque et les Agents de support, enregistre les informations concernant les éléments sauvegardés, gère les supports et exécute d'autres fonctions similaires.

Inet	Le service Inet Data Protector s'exécute sur chaque système Windows de la cellule Data Protector. Inet est responsable de la communication entre les systèmes de la cellule et lance les processus requis pour les sauvegardes et les restaurations. Le service Inet Data Protector est lancé dès que Data Protector est installé sur un système. Sur les systèmes UNIX, le démon inet système (INETD) lance le processus Inet Data Protector.
CRS	Le processus (service) CRS (Cell Request Server) s'exécute sur le Gestionnaire de cellule Data Protector. Il lance et contrôle les sessions de sauvegarde et de restauration. Le service est lancé dès que Data Protector est installé sur le système Gestionnaire de cellule. Il est relancé chaque fois que le système est redémarré.
MMD	Le processus (service) MMD (Media Management Daemon, démon de gestion des supports), s'exécute sur le Gestionnaire de cellule Data Protector et contrôle les opérations liées aux périphériques et à la gestion des supports. Il est lancé par le processus (service) CRS.
RDS	Le processus RDS (Raima Database Server, serveur de base de données Raima) s'exécute sur le Gestionnaire de cellule Data Protector et gère la base de données IDB. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.

Pour savoir comment lancer ou arrêter manuellement les processus et services Data Protector, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector* ou à l'aide en ligne.

Sessions de sauvegarde

Cette section explique comment lancer une session de sauvegarde et décrit le déroulement d'une session de ce type, ainsi que les processus et services impliqués.

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

Dès qu'une spécification de sauvegarde est lancée, elle devient une session de sauvegarde. Au cours d'une session de sauvegarde, les données d'une source, généralement un disque dur, sont copiées vers une destination, généralement un support à bande. Le résultat d'une session de sauvegarde est une copie de données sur une série de supports de sauvegarde.

Sessions de sauvegarde interactives ou planifiées

Session de sauvegarde planifiée

Une session de sauvegarde planifiée est lancée par le planificateur Data Protector à l'heure spécifiée. Vous pouvez suivre l'évolution de la session dans le moniteur Data Protector.

Session de sauvegarde interactive

Une session de sauvegarde interactive est lancée directement depuis l'interface utilisateur Data Protector. Le moniteur Data Protector démarre immédiatement et vous pouvez alors suivre l'évolution de la session de sauvegarde. Notez que plusieurs utilisateurs peuvent suivre une même session de sauvegarde. Vous pouvez arrêter le contrôle en déconnectant l'interface utilisateur de la session. La session continuera alors en arrière-plan.

Flux de données et processus d'une session de sauvegarde

Déroulement d'une session de sauvegarde

Le flux d'informations d'une session de sauvegarde est présenté dans la figure 7-1 à la page 258. Notez que le flux de données et les processus décrits dans cette section sont ceux d'une session de sauvegarde réseau standard. Pour une présentation du flux de données et des processus spécifiques d'autres types de sauvegarde, tels que les sauvegardes directes, reportez-vous aux chapitres correspondants.

Au démarrage d'une session de sauvegarde, les événements suivants se produisent :

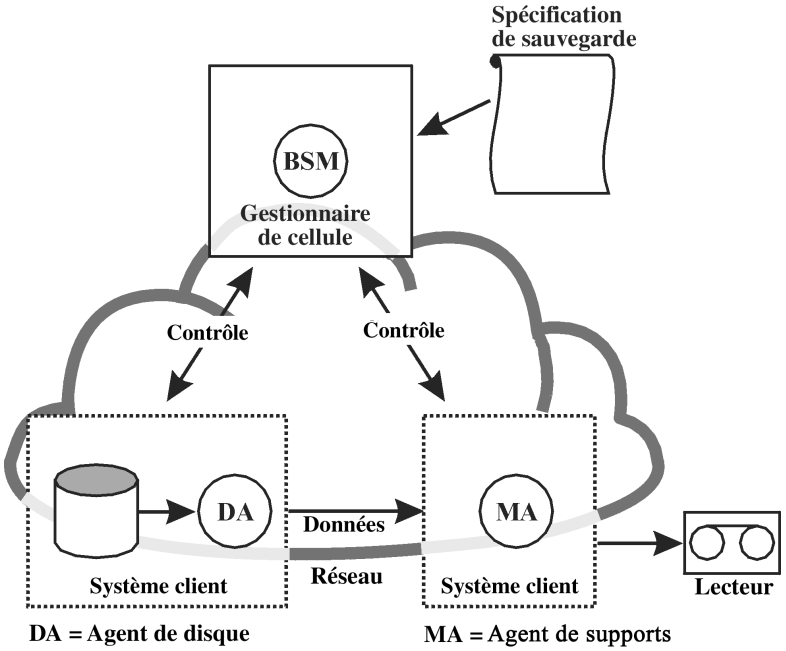
1. Le processus BSM (Backup Session Manager, gestionnaire de session de sauvegarde) est lancé à partir du système Gestionnaire de cellule et contrôle la session de sauvegarde. Il lit la spécification de sauvegarde pour déterminer les éléments à sauvegarder, ainsi que les options, les supports et les périphériques à utiliser pour la sauvegarde.
2. Le BSM (Backup Session Manager, gestionnaire de session de sauvegarde) ouvre la base de données IDB et y écrit les informations concernant la session de sauvegarde : messages générés, informations concernant les données sauvegardées, périphériques et supports utilisés pour la session.
3. Le BSM lance des Agents de support sur les systèmes associés aux périphériques configurés pour la sauvegarde. Un Agent de support est lancé pour chaque lecteur utilisé en parallèle. Le nombre d'Agents de support pouvant être lancés dans la cellule est limité par la configuration de la cellule et par le nombre de licences que vous avez achetées.

   Dans une session de sauvegarde avec mise en miroir d'objet, le gestionnaire BSM lance également les Agents de support qui seront utilisés pour la mise en miroir.
4. Le BSM lance un Agent de disque pour chaque disque à sauvegarder en parallèle. Le nombre effectif d'Agents de disque qu'il est possible de lancer dépend de la simultanéité des Agents de disque, telle qu'elle a été définie au niveau de la spécification de sauvegarde. La simultanéité correspond au nombre d'Agents de disque pouvant être lancés simultanément de sorte que les données soient envoyées en parallèle à un Agent de support et que le périphérique puisse fonctionner en mode continu.
5. Les Agents de disque lisent les données des disques et les transmettent aux Agents de support qui les écrivent sur des supports.

   Dans une session de sauvegarde avec mise en miroir d'objet, les Agents de support utilisés pour l'écriture des objets mis en miroir forment une guirlande. Chaque Agent de support écrit les données reçues sur le support et les transmet à l'Agent de support suivant dans la chaîne.

6. Le BSM contrôle l'avancement de la session et lance des Agents de disque et des Agents de support supplémentaires en fonction des besoins.
7. Enfin, BSM ferme la session lorsqu'elle est terminée.

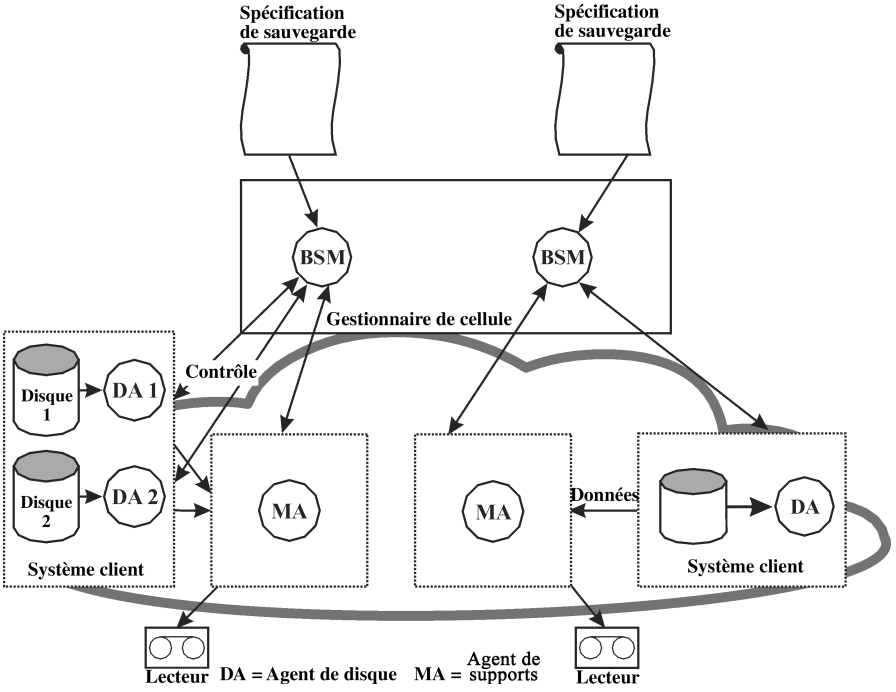
Figure 7-1 Flux de données de la session de sauvegarde (1)



Nombre de sessions pouvant être lancées simultanément

Un certain nombre de sessions peuvent être lancées simultanément dans la cellule, comme indiqué à la figure 7-2. Ce nombre dépend des ressources de la cellule, notamment de la configuration du Gestionnaire de cellule : vitesse du processeur, taille de la mémoire principale, espace disque et autres données du même type. Vous pouvez configurer le nombre maximum de sessions de sauvegarde pouvant être exécutées simultanément.

Figure 7-2 **Flux de données d'une session de sauvegarde - sessions multiples**



Commandes pré-exécution et post-exécution

Les commandes Data Protector pré-exécution permettent d'effectuer certaines opérations avant qu'une session de sauvegarde ou de restauration ne commence. Les commandes Data Protector post-exécution permettent d'effectuer certaines opérations au terme d'une session de sauvegarde ou de restauration. Exemple d'opération pré-exécution type : fermer la base de données pour mettre les données dans un état cohérent.

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

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

File d'attente des sessions de sauvegarde

Délai d'attente

Au démarrage d'une session de sauvegarde, Data Protector tente d'allouer toutes les ressources nécessaires, telles que les périphériques. La session est mise en attente jusqu'à ce que les ressources minimales requises soient disponibles. Si les ressources ne sont toujours pas disponibles au terme de ce délai, la session est abandonnée. Le délai d'attente peut être défini à l'aide de l'option globale `SmWaitForDevice`.

Optimisation de la charge

Pour optimiser la charge du système Gestionnaire de cellule, Data Protector peut lancer un certain nombre de sessions de sauvegarde en même temps. Ce nombre est égal à 5 par défaut et peut être modifié au niveau du fichier d'options globales. Si le nombre de sessions planifiées devant être lancées simultanément est supérieur au nombre par défaut, les sessions supplémentaires sont mises en file d'attente et lancées une fois les autres terminées.

Demandes de montage au cours d'une session de sauvegarde

Qu'est-ce qu'une demande de montage ?

Une demande de montage apparaît au cours d'une session de sauvegarde lorsque Data Protector requiert un support supplémentaire pour effectuer la sauvegarde et que celui-ci n'est pas disponible.

Data Protector peut émettre une demande de montage pour l'un des motifs suivants :

Emission d'une demande de montage

- L'espace de supports de sauvegarde est insuffisant et aucun support supplémentaire n'est disponible.
- La stratégie d'allocation de supports Data Protector définie requiert un support qui n'est pas présent dans le périphérique.
- Les supports utilisés pour la sauvegarde ne sont pas disponibles dans l'ordre défini au niveau de la liste de préallocation.

Pour plus d'informations, reportez-vous aux sections "Ajout de données aux supports pendant une session de sauvegarde" à la page 152 et "Sélection des supports utilisés pour la sauvegarde" à la page 151.

Réponse à une demande de montage

Répondre à une demande de montage consiste à fournir les supports requis et à demander à Data Protector de continuer la sauvegarde.

Data Protector permet de définir les opérations devant être effectuées en cas d'émission d'une demande de montage :

Envoi d'une notification à un opérateur

Vous pouvez configurer une notification Data Protector pour que l'opérateur reçoive un e-mail contenant les informations relatives à la demande de montage. L'opérateur peut dans ce cas prendre les mesures appropriées, par exemple charger manuellement le support requis ou abandonner la session. Pour plus d'informations, reportez-vous à la section "Génération de rapports et notification" à la page 240.

Automatisation d'une demande de montage

Vous pouvez configurer des opérations automatisées destinées à traiter les demandes de montage. Pour cela, rédigez un script ou un programme de commandes permettant d'effectuer les actions souhaitées.

Sauvegarde en mode détection de disques

Qu'est-ce que la détection de disque ?

Lors d'une sauvegarde en mode détection de disques, Data Protector crée une liste détaillée des disques présents sur le système cible une fois la session de sauvegarde lancée, et sauvegarde tous ces disques. Ainsi, tous les disques locaux présents sur le système sont sauvegardés, même s'ils ne figuraient pas sur le système au moment de la configuration de la sauvegarde. La sauvegarde en mode détection des disques est particulièrement utile dans les environnements dynamiques dont les configurations changent rapidement. Elle permet de sélectionner ou d'exclure des répertoires spécifiques dans la sauvegarde.

Comparaison avec une sauvegarde standard

Dans le cas d'une sauvegarde standard, vous configurez la sauvegarde en définissant explicitement des disques, des répertoires et d'autres objets spécifiques dans la spécification de sauvegarde. Ces objets sont les seuls sauvegardés. Si vous ajoutez des disques au système ou si vous souhaitez sauvegarder d'autres objets, vous devez modifier manuellement la spécification de sauvegarde ainsi que les nouveaux objets. Lorsque vous configurez la sauvegarde, vous pouvez sélectionner la méthode à utiliser : sauvegarde en mode détection de disques ou en mode standard.

Sessions de copie d'objet

Cette section explique comment lancer une session de copie et décrit le déroulement d'une session de ce type, ainsi que les processus et services impliqués.

Qu'est-ce qu'une session de copie d'objet ?

Une session de copie d'objet est un processus qui crée une copie supplémentaire des données sauvegardées sur un jeu de supports différent. Pendant une session de copie d'objet, les objets sauvegardés sélectionnés sont copiés à partir de la source vers le support cible.

Sessions automatiques et interactives de copie d'objet

Session automatique de copie d'objet

Une session automatique de copie d'objet peut être planifiée ou lancée immédiatement après une sauvegarde. Une session planifiée de copie d'objet démarre à l'heure que vous avez spécifiée à l'aide du planificateur Data Protector. Une session de copie d'objet après sauvegarde débute une fois la session de sauvegarde spécifiée terminée. Vous pouvez suivre l'évolution de la session automatique de copie d'objet dans le moniteur Data Protector.

Session interactive de copie d'objet

Une session de copie d'objet interactive est lancée directement depuis l'interface utilisateur Data Protector. Le moniteur Data Protector démarre immédiatement et vous pouvez alors suivre l'évolution de la session. Plusieurs utilisateurs peuvent contrôler la même session de copie d'objet. Vous pouvez arrêter le contrôle en déconnectant l'interface utilisateur de la session. La session continuera alors en arrière-plan.

Flux de données et processus d'une session de copie d'objet

Que se passe-t-il au cours d'une session de copie d'objet ?

Le flux d'informations d'une session de copie d'objet est présenté dans la figure 7-3 à la page 264. Au démarrage d'une session de copie d'objet, les événements suivants se produisent :

1. Le processus CSM (Copy Session Manager, gestionnaire de session de copie) est lancé sur le système Gestionnaire de cellule. Ce processus lit les spécifications de la copie d'objet en recherchant les

informations relatives aux objets qui doivent être copiés ainsi qu'aux options, supports et périphériques à utiliser. Il contrôle également la session de copie d'objet.

2. Le CSM ouvre la base de données IDB, lit les données relatives aux supports requis pour la copie et écrit les informations concernant la session de copie d'objet, par exemple les messages générés.
3. Le CSM verrouille les Agents de support. La session est mise en attente jusqu'à ce que tous les Agents de support de lecture et les Agents de support d'écriture requis soient verrouillés, le délai d'attente étant le même que pour la sauvegarde. Si les ressources ne sont toujours pas disponibles au terme du délai d'attente, la session est abandonnée.
4. Le CSM lance les Agents de support sur les systèmes possédant des périphériques configurés pour la copie. Les Agents de support reçoivent les supports source et cible alloués en fonction des stratégies de sauvegarde.
5. Les Agents de support lisent les données dans les supports source et se connectent aux Agents de support porteurs des supports cible.

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

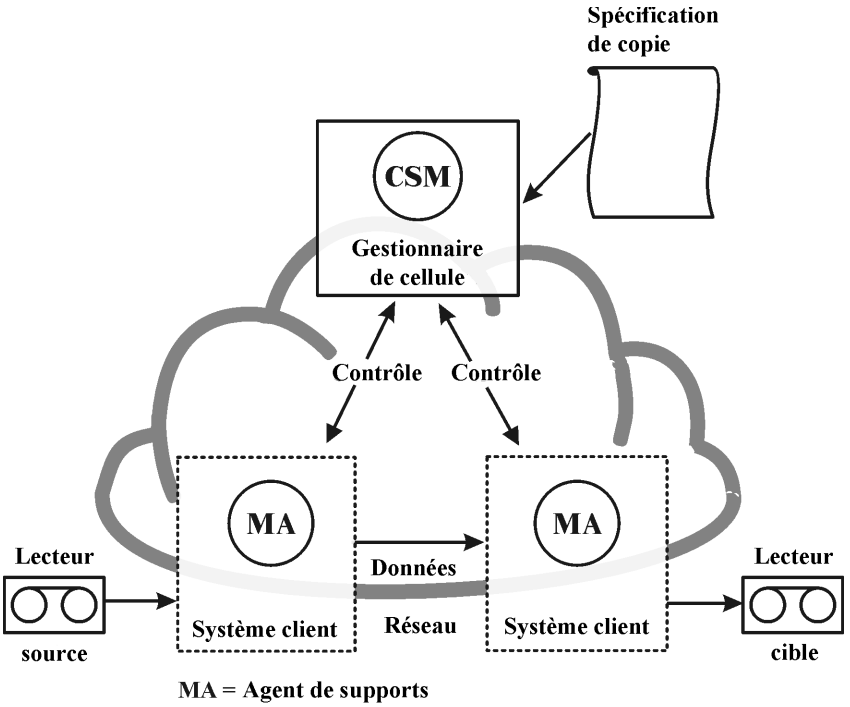
   - Les périphériques de destination ayant la même taille de bloc que les périphériques source sont sélectionnés avant ceux dont la taille de bloc diffère.
   - Les périphériques connectés localement sont sélectionnés avant les périphériques en réseau.
6. Les Agents de support porteurs des supports cible acceptent les connexions provenant des Agents de support porteurs des supports source et commencent à écrire les copies d'objet sur les supports cible.

   Si la taille de bloc du périphérique source est inférieure à la taille de bloc du périphérique de destination, les blocs sont redimensionnés à ce stade de la session de copie d'objet.
7. Le CSM ferme la session de copie d'objet lorsqu'elle est terminée.

Nombre de sessions pouvant être lancées simultanément

Un certain nombre de sessions de copie d'objet peuvent s'exécuter simultanément dans la cellule. Ce nombre dépend des ressources de la cellule : Gestionnaire de cellule et les systèmes associés aux périphériques connectés.

Figure 7-3 Flux d'informations d'une session de copie d'objet



Mise en file d'attente des sessions de copie d'objet

Délai d'attente

Lorsqu'une session de copie d'objet débute, Data Protector essaie d'allouer toutes les ressources nécessaires. La session est mise en attente jusqu'à ce que les ressources minimales requises soient disponibles. Si les ressources ne sont toujours pas disponibles au terme du délai d'attente, la session est abandonnée. Le délai d'attente peut être défini à l'aide de l'option globale `SmWaitForDevice`.

Demandes de montage dans une session de copie d'objet

Qu'est-ce qu'une demande de montage ?

Une demande de montage dans une session de copie d'objet est émise lorsqu'un support source ou cible nécessaire pour l'opération de copie d'objet n'est pas disponible.

Réponse à une demande de montage

La réponse à une demande de montage inclut la fourniture du support requis et la confirmation de la demande de montage. Si le support source requis dispose de copies de supports, vous pouvez fournir une copie à la place du suppoort d'origine.

Sessions de restauration

Cette section explique comment lancer une session de restauration et décrit le déroulement d'une session de ce type, ainsi que les processus et services impliqués.

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

Lors d'une session de restauration, Data Protector extrait les données d'une copie de sauvegarde, généralement un support à bande, pour les transférer sur un disque.

Une session de restauration est lancée de manière interactive. Vous devez tout d'abord indiquer à Data Protector les éléments à restaurer. Les supports requis sont ensuite automatiquement sélectionnés. Enfin, vous devez définir certaines options et lancer la restauration. L'avancement de la session peut être suivi par la personne ayant lancé la session, mais aussi par d'autres utilisateurs.

Flux de données et processus d'une session de restauration

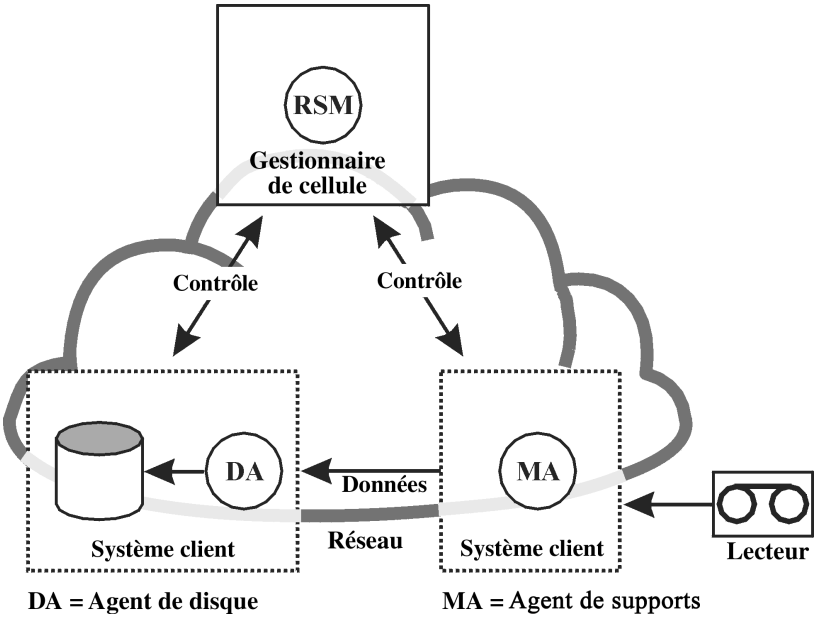
Déroulement d'une session de restauration

Lorsqu'une session de restauration est lancée, comme illustré à la figure 7-4, les événements suivants se produisent :

1. Le processus RSM (Restore Session Manager, gestionnaire de session de restauration) est lancé sur le système Gestionnaire de cellule. Ce processus contrôle la session de restauration.
2. Le RSM ouvre la base de données IDB, lit les données relatives aux supports requis pour la restauration et écrit les informations concernant la session de restauration, par exemple les messages générés.
3. Le RSM lance les Agents de support sur les systèmes associés aux périphériques utilisés pour la restauration. Le RSM lance un Agent de support pour chaque lecteur utilisé en parallèle.
4. Le RSM lance un Agent de disque (AD) pour chaque disque restauré en parallèle. Le nombre d'Agents de disque pouvant être lancés simultanément dépend des objets sélectionnés en vue de la restauration. Pour plus d'informations, reportez-vous à la section "Restaurations parallèles" à la page 268.

5. Les Agents de support lisent les données des supports et les transmettent aux Agents de disque qui les écrivent sur des disques. Le RSM contrôle l'avancement de la session et lance des Agents de disque et des Agents de support supplémentaires en fonction des besoins.
6. Le RSM ferme la session lorsqu'elle est terminée.

Figure 7-4 Flux de données d'une session de restauration



Nombre de sessions de restauration pouvant être lancées simultanément

Un certain nombre de sessions peuvent être lancées simultanément dans la cellule. Ce nombre dépend des ressources de la cellule : Gestionnaire de cellule, systèmes associés aux périphériques connectés, etc.

File d'attente des sessions de restauration

Délai d'attente

Au démarrage d'une session de sauvegarde, Data Protector tente d'allouer toutes les ressources nécessaires, telles que les périphériques. La session reste en file d'attente tant que les ressources minimales requises ne sont pas disponibles. Data Protector tente d'allouer les

ressources pendant une période spécifique : le délai d'attente. Vous pouvez configurer ce dernier. Si les ressources ne sont toujours pas disponibles au terme du délai d'attente, la session est abandonnée.

Demandes de montage au cours d'une session de restauration

Qu'est-ce qu'une demande de montage ?

Une demande de montage apparaît au cours d'une session de restauration lorsque les supports requis en vue de la restauration ne sont pas disponibles dans le périphérique. Data Protector permet de définir les opérations devant être effectuées en cas d'émission d'une demande de montage.

Réponse à une demande de montage

Répondre à une demande de montage consiste à fournir le support requis, ou toute copie du support, et à demander à Data Protector de continuer la restauration.

Restaurations parallèles

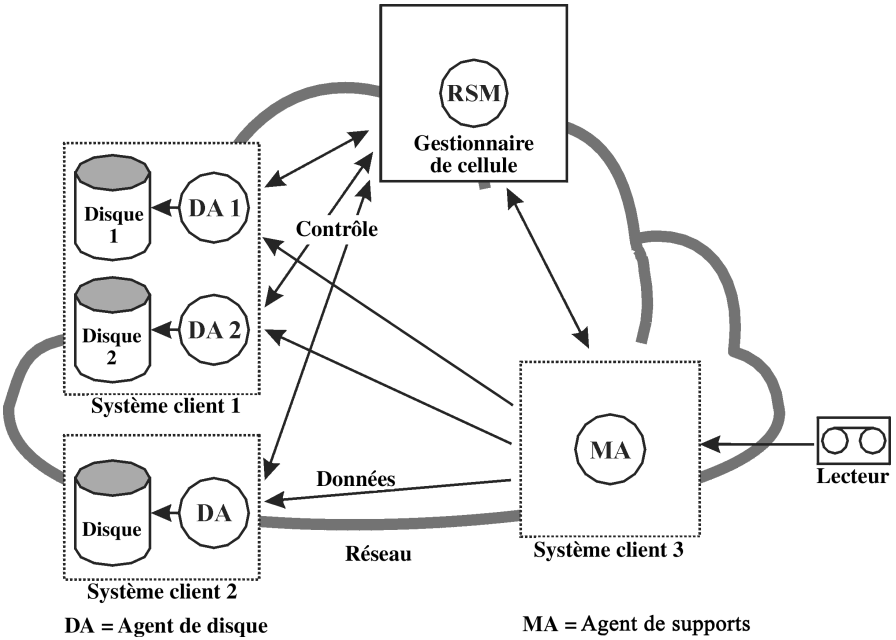
Qu'est-ce qu'une restauration parallèle ?

Lors d'une restauration parallèle, des données entrelacées issues de différents objets sont lues simultanément à partir d'un support, selon un chemin unique, puis sont restaurées. La restauration parallèle améliore les performances de façon significative lorsqu'il s'agit de restaurer plusieurs objets à partir du même support. Pour plus d'informations, reportez-vous à la figure 7-5.

Comparaison avec une restauration standard

Les données issues des différents Agents de disque sont (dans la plupart des cas) multiplexées et stockées sur le support. Reportez-vous à la section "Sessions et objets multiples par support, écritures simultanées" à la page 153. Lors d'une restauration standard, Data Protector lit les données multiplexées sur le support et rassemble uniquement les parties requises pour l'objet sélectionné. Lors de la restauration de l'objet suivant, Data Protector doit rembobiner le support et lire les parties correspondant à cet autre objet, en supposant que les deux objets se trouvent sur le même support et ont été écrits par multiplexage.

Figure 7-5 Flux de session d'une restauration parallèle



Lors d'une restauration parallèle, Data Protector lit les données multiplexées pour tous les objets sélectionnés et rassemble à la volée les parties requises pour chacun d'entre eux, en transmettant les données aux Agents de disque appropriés. Les performances en termes de lecture du support sont ainsi améliorées. Les performances en termes d'écriture sur disques sont également optimisées si les objets sélectionnés doivent être écrits sur plusieurs disques physiques différents : dans ce cas, les données sont copiées sur plusieurs disques en même temps.

Restauration rapide de plusieurs fichiers individuels

Data Protector utilise la fonctionnalité de restauration d'objets non contigus pour améliorer les performances de restauration. Après avoir restauré un fichier ou une arborescence, Data Protector se repositionne directement au niveau de l'arborescence ou du fichier suivant sur le support, si les fichiers ou les arborescences sont séparés au minimum par un segment, et continue la restauration.

Vous pouvez lancer plusieurs Agents de disque pour un objet restauration individuel. De cette manière, la restauration de plusieurs fichiers individuels situés à différents emplacements du support est beaucoup plus rapide que si Data Protector devait parcourir ce dernier.

Sessions de gestion des supports

Qu'est-ce qu'une session de gestion des supports ?

Il s'agit d'une session servant à exécuter une action sur les supports, comme l'initialisation, l'analyse de contenu, la vérification des données stockées sur les supports et la copie de supports.

Connexion à la base de données IDB

Les informations relatives à une session de gestion des supports, notamment les messages générés, sont stockées dans la base de données IDB.

Suivi de la session de gestion des supports dans le moniteur Data Protector

Il est possible de visualiser une session de gestion des supports dans la fenêtre de contrôle. Si vous fermez l'interface utilisateur de Data Protector, la session se poursuit en arrière-plan.

Flux de données d'une session de gestion des supports

Déroulement d'une session de gestion des supports

Lorsqu'une session de gestion des supports est lancée, les événements suivants se produisent :

1. Le processus MSM (Media Session Manager, gestionnaire de session de supports) est lancé sur le système Gestionnaire de cellule. Ce processus contrôle la session de gestion des supports.
2. Le MSM lance les Agents de support sur le système associé aux périphériques utilisés pour la session de gestion des supports.
3. Les Agents de support exécutent l'opération demandée et envoient les messages générés à l'interface utilisateur Data Protector, celle-ci permettant de suivre l'évolution de la session. La session est également stockée dans la base de données IDB.
4. Le MSM ferme la session lorsqu'elle est terminée.

Nombre de sessions pouvant être exécutées simultanément

Un certain nombre de sessions de gestion des supports peuvent être exécutées simultanément dans la cellule si ces sessions n'utilisent pas les mêmes ressources (périphériques, supports, etc.).

8 Intégration avec les applications de base de données

Description du chapitre

Ce chapitre contient une brève description de l'intégration de Data Protector avec les applications de base de données, telles que Microsoft Exchange Server, Oracle et Informix OnLine Server.

Il s'organise comme suit :

"Présentation d'une base de données" à la page 273

"Sauvegarde de systèmes de fichiers de bases de données et d'applications" à la page 276

"Sauvegarde en ligne de bases de données et d'applications" à la page 277

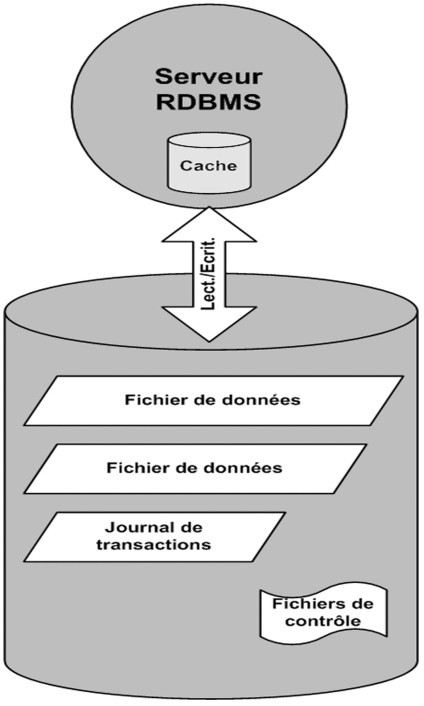
Pour connaître la liste détaillée des intégrations prises en charge, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.

Présentation d'une base de données

Du point de vue de l'utilisateur, une **base de données** est un ensemble de données. Les données d'une base sont stockées dans des **tables**. Les tables relationnelles sont définies par leurs colonnes ; un nom leur est attribué. Les données sont enregistrées dans les lignes de la table. Les tables peuvent être reliées entre elles et la base de données peut être utilisée pour mettre en application ces liaisons. Les données peuvent donc être enregistrées dans un **format relationnel** ou sous des structures **orientées objet** comme les méthodes et les types de données abstraits. Les objets peuvent être reliés à d'autres objets et contenir d'autres objets. Une base de données est généralement gérée par le processus serveur (gestionnaire), qui maintient l'intégrité et la cohérence des données.

Que vous utilisiez les structures relationnelles ou celles orientées objet, les données d'une base sont stockées dans des **fichiers**. En interne, il s'agit de structures de base de données qui établissent un mappage logique entre des données et des fichiers, permettant de stocker séparément des types de données différents. On appelle ces divisions logiques des **espaces de table** dans Oracle, des **dbspaces** dans INFORMIX Online, et des **segments** dans Sybase.

Figure 8-1 Base de données relationnelle



La figure 8-1 présente une base de données relationnelle type qui comporte les structures décrites ci-dessous.

Les **fichiers de données** contiennent physiquement l'ensemble des données d'une base de données. Ils changent de manière aléatoire et peuvent être très volumineux. Un fichier de données est divisé en pages.

Dans les **journaux de transactions**, toutes les transactions des bases de données sont enregistrées avant la suite de leur traitement. Si un échec empêche l'écriture définitive de données modifiées dans un fichier de données, les modifications peuvent être obtenues à partir d'un fichier journal. La récupération, quelle qu'elle soit, s'effectue en deux étapes : la phase **"roll forward"**, au cours de laquelle les modifications des transactions sont appliquées dans la base de données principale, et la phase **"roll back"**, durant laquelle les transactions non validées sont supprimées.

Les **fichiers de contrôle** contiennent des informations sur la structure physique des bases de données, par exemple leur nom, les noms et emplacements de leurs fichiers de données et fichiers journaux, ainsi que l'horodatage de leur création. Ces données de contrôle sont conservées dans les fichiers de contrôle, lesquels sont essentiels au bon fonctionnement de la base de données.

La **mémoire cache** du processus serveur de base de données contient les pages les plus fréquemment utilisées des fichiers de données.

La procédure suivante représente le flux standard du traitement d'une transaction :

1. Une transaction est d'abord enregistrée dans le journal de transactions.
2. Les modifications requises dans la transaction sont ensuite appliquées aux pages mises en cache.
3. De temps à autre, des groupes de pages modifiées sont transférés dans des fichiers de données se trouvant sur le disque.

Sauvegarde de systèmes de fichiers de bases de données et d'applications

Les bases de données changent constamment lorsqu'elles sont connectées. Un serveur de base de données est constitué de plusieurs composants, lesquels permettent de réduire le temps de réponse aux utilisateurs connectés et d'améliorer les performances. Certaines données sont conservées dans la mémoire cache interne, et d'autres dans des fichiers journaux temporaires qui sont transférés à des **points de contrôle**.

Les données d'une base pouvant changer au cours d'une sauvegarde, une sauvegarde de système de fichiers de base de données n'a pas de sens si le serveur de base de données n'est pas mis dans un mode spécial ou même hors ligne. Les fichiers de bases de données enregistrés doivent se trouver dans un état cohérent, sinon les données sont inutilisables.

Il est nécessaire de respecter la procédure suivante pour configurer la sauvegarde d'un système de fichiers de base de données ou d'application :

- Identifiez tous les fichiers de données.
- Préparez deux programmes, l'un capable de fermer la base de données, l'autre de l'ouvrir.
- Configurez la **spécification de sauvegarde** du système de fichiers avec tous ses fichiers de données, puis indiquez le programme de fermeture comme étant une **commande pré-exécution** et le programme d'ouverture comme étant une **commande post-exécution**.

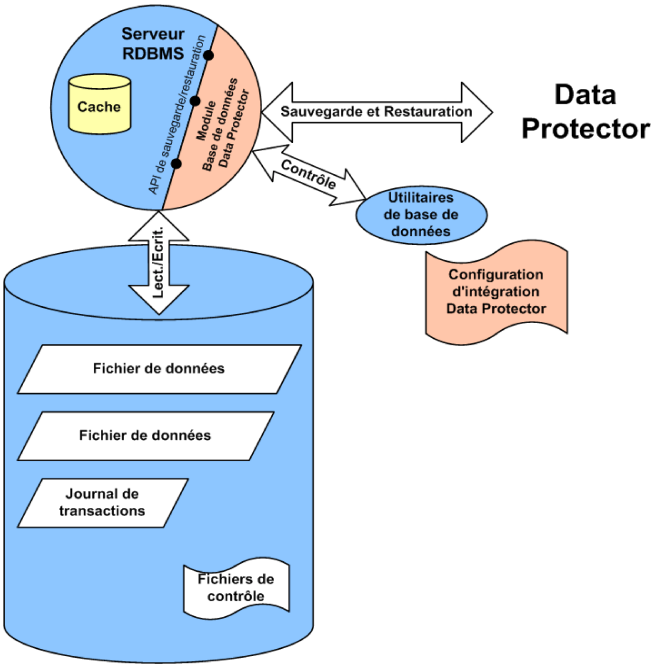
Cette méthode est assez simple à comprendre et à appliquer, mais possède un inconvénient majeur : *la base de données n'est pas accessible pendant la sauvegarde*, ce qui est inacceptable pour la plupart des environnements professionnels.

Sauvegarde en ligne de bases de données et d'applications

Pour pallier la nécessité de fermer la base de données pendant une sauvegarde, les fournisseurs de bases de données ont mis au point des interfaces permettant de mettre provisoirement la base de données dans un mode spécial afin d'enregistrer les données sur bandes. Les applications serveur restent donc connectées et accessibles par les utilisateurs durant le processus de sauvegarde ou de restauration. Grâce à ces interfaces spécifiques aux applications, il est possible de sauvegarder ou de restaurer des unités logiques de l'application de base de données à l'aide de produits de sauvegarde tels que Data Protector. Les fonctionnalités des API de sauvegarde varient en fonction des fournisseurs de base de données. Les principales bases de données et applications s'intègrent avec Data Protector. Pour obtenir une liste détaillée des intégrations prises en charge, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*

L'interface de sauvegarde a pour fonction de fournir des données cohérentes (même si elles ne le sont pas sur disque) à l'application de sauvegarde, tout en laissant la base de données opérationnelle.

Figure 8-2 Intégration de Data Protector avec les bases de données



La figure 8-2 présente l'intégration d'une base de données relationnelles avec Data Protector. Data Protector fournit une **bibliothèque de base de données** qui est reliée au serveur de base de données. Le serveur de base de données envoie et demande des données à Data Protector. Les utilitaires de base de données sont utilisés pour déclencher les opérations de sauvegarde et de restauration.

Les étapes suivantes constituent une procédure standard pour configurer la sauvegarde d'une base de données avec l'intégration de Data Protector :

1. Un agent spécifique de base de données/d'application est installé sur le système de base de données.
2. L'intégration de Data Protector est configurée pour chaque base de données. Les données nécessaires à Data Protector pour travailler avec cette base de données sont stockées dans le système de base de données (dans des entrées de registre ou des fichiers de configuration). En général, il s'agit notamment de chemins d'accès et de noms/mots de passe d'utilisateurs.

3. La spécification de sauvegarde est préparée à l'aide de l'interface utilisateur de Data Protector.

La base de données reste **en ligne** sans interruption, ce qui constitue un avantage considérable ; en outre, l'utilisation de l'intégration de Data Protector avec les bases de données présente d'autres avantages :

- Il n'est pas nécessaire de spécifier l'emplacement des fichiers de données. Ces derniers peuvent se trouver sur des disques différents.
- Il est possible d'explorer la structure logique de la base de données. Vous pouvez également sélectionner un seul sous-ensemble de la base de données.
- En cas de sauvegarde, les applications sont informées et contrôlent les éléments sauvegardés.
- Plusieurs modes de sauvegarde sont possibles. Outre les sauvegardes **complètes**, les utilisateurs peuvent sélectionner des sauvegardes (niveau de bloc) **incrémentales**, ou uniquement la sauvegarde de fichiers journaux de transactions.
- Plusieurs modes de restauration sont possibles et, après la restauration de fichiers de données, la base de données peut automatiquement restaurer des journaux de transactions et les appliquer selon leur configuration.

9 Sauvegarde directe

Description du chapitre

Le présent chapitre présente le concept de sauvegarde directe ainsi que les technologies associées. Il décrit également les configurations de sauvegarde directe prises en charge par Data Protector.

Il s'organise comme suit :

"Présentation" à la page 283

"Caractéristiques requises et éléments pris en charge" à la page 291

"Configurations prises en charge" à la page 292

Présentation

Actuellement, on enregistre une demande croissante de solutions de sauvegarde réduisant le temps d'indisponibilité des applications et l'encombrement des systèmes tout en augmentant la vitesse de sauvegarde. Le volume des données grimpe également : il a doublé tous les 18 mois ces 20 dernières années et continue de progresser à un rythme encore plus rapide.

Les applications et les services doivent être accessibles en ligne presque à tout moment et offrir des performances maximales. Les fenêtres de sauvegarde sont étroites et la dégradation des performances due aux opérations de sauvegarde (ou à toute autre opération) n'est plus acceptable.

En outre, les solutions n'exigeant pas d'investissements importants dans des équipements spécifiques font aussi l'objet d'une demande croissante.

Ces besoins divers ont entraîné le développement et l'introduction de nouvelles technologies de sauvegarde directe ou "sans serveur".

Pour les entreprises et les fournisseurs de services gérant des environnements Oracle stratégiques, la fonction de sauvegarde directe de Data Protector est une extension non intrusive de la gamme HP de solutions de sauvegarde réseau.

La sauvegarde directe étend les avantages de la solution ZDB de HP en transférant directement les données du disque vers la bande et en minimisant l'encombrement du serveur de sauvegarde, voire en rendant son utilisation facultative.

Elle limite l'impact sur les serveurs de production de bases de données par l'utilisation de technologies de miroirs basées sur le matériel plutôt que de snapshots intrusifs basés sur le logiciel.

En outre, la solution de sauvegarde directe est entièrement compatible avec la commande standard XCopy (ANSI T10 SCP-2 Extended Copy Standard), elle-même incorporée dans les bibliothèques de bande HP StorageWorks (ainsi que dans les passerelles Fibre channel SCSI externes), éliminant ainsi la nécessité de recourir à un dispositif distinct de déplacement des données ("data mover").

REMARQUE Pour obtenir une liste des applications, systèmes d'exploitation et périphériques pris en charge par la sauvegarde directe dans HP OpenView Storage Data Protector A.05.50, reportez-vous à la section "Configurations prises en charge" à la page 292.

Sauvegarde directe

Qu'est-ce qu'une sauvegarde directe ? Il s'agit d'une méthode de sauvegarde "sans serveur", c'est-à-dire n'utilisant pas de serveur de sauvegarde dédié pour déplacer les données. Celles-ci ne transitent pas via le réseau local, mais sont *directement* envoyées du système client vers un périphérique à bandes où elles sont sauvegardées.

La sauvegarde directe peut concerner des fichiers de données d'application, des fichiers de contrôle et des images disque (disque brut ou volume logique brut).

La sauvegarde directe utilise les technologies Split Mirror et SAN (Storage Area Network) existantes pour :

- Accéder aux données d'application en exerçant un impact minimal sur l'application ; le serveur d'application n'est guère sollicité (ce qui entraîne un temps d'indisponibilité de l'application nul ou très réduit).
- Déplacer les données sans être confronté aux goulets d'étranglement associés au trafic réseau et au débit du réseau local.

Afin de prendre en charge les sauvegardes directes/sans serveur, Data Protector incorpore aussi une nouvelle technologie destinée à résoudre les systèmes de fichiers cible et à déplacer les données sur le SAN. Cette nouvelle technologie, basée sur la norme XCopy, offre une méthode pour déplacer les données du système cible vers le périphérique à bandes sans les faire passer par un serveur. Pour une courte présentation de XCopy, reportez-vous à la section "A propos de XCopy" à la page 288.

Ce cheminement direct des données du disque vers la bande (via le SAN) aide à réduire la nécessité d'investir dans des équipements et à augmenter l'utilisation des infrastructures existantes.

Types de sauvegarde

La sauvegarde directe peut concerner des fichiers de données d'application, des fichiers de contrôle et des images disque (disque brut ou volume logique brut).

Avantages de la sauvegarde directe

Le data mover se trouvant dans la passerelle SAN et la technologie qui interprète le système cible étant intégrée à l'Agent général de supports, les utilisateurs de la sauvegarde directe peuvent avoir recours à un serveur de gestion économique pour piloter la sauvegarde et éviter d'investir dans de multiples serveurs pour réaliser l'identification des blocs.

La sauvegarde directe permet en outre d'augmenter les capacités matérielles afin d'accroître le temps de bon fonctionnement d'une part, et d'améliorer les capacités de restauration instantanée afin de réduire le temps de restauration d'autre part.

La sauvegarde directe ne se limite pas aux systèmes de fichiers propriétaires ni aux LVM.

La sauvegarde directe accroît la valeur de votre solution de sauvegarde à de nombreux égards. Ainsi, la sauvegarde directe :

- Tire parti des fonctions XCopy les plus avancées afin d'accélérer les opérations de sauvegarde.
- Augmente considérablement le temps de bon fonctionnement en améliorant les capacités de mise en miroir matérielle et de snapshot.
- Permet d'accéder à la fonction inégalée de restauration instantanée de Data Protector afin d'accélérer la récupération.
- N'exige que très peu de ressources processeur et mémoire de la part du périphérique hôte XCopy.

Fonctionnement de la sauvegarde directe

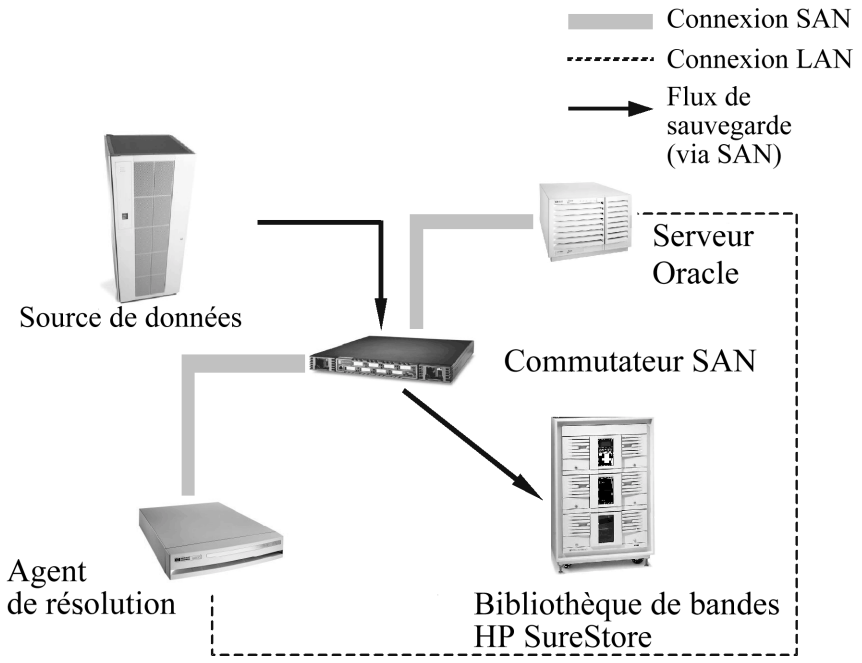
Comme pour tout autre type de sauvegarde Data Protector, vous créerez une spécification de sauvegarde définissant quand et comment la sauvegarde doit avoir lieu.

- L'Agent général de supports sur le serveur d'application met en attente l'application.
- L'agent Split Mirror sur le serveur d'application et l'hôte de sauvegarde crée des copies miroir.

- L'Agent général de supports sur l'hôte de sauvegarde :
  - — Résout le disque du système cible.
  - — Calcule les informations de résolution.
  - — Appelle XCopy.
- Ensuite, XCopy extrait les données cible et les transfère au périphérique à bandes via la passerelle.

La figure 9-1 représente une configuration de base pour la sauvegarde directe. Selon cette configuration, l'agent Resolve se trouve sur un hôte de sauvegarde distinct. Toutefois, les données ne transitent pas par cet hôte.

Figure 9-1 Architecture de sauvegarde directe



Environnement

Cette section décrit l'environnement de sauvegarde directe, à savoir les périphériques à raccorder ainsi que les éléments auxquels ils doivent être raccordés. Elle présente également les agents requis et l'endroit où ils sont installés.

Pour plus d'informations sur les plates-formes, les lecteurs de bande et les bibliothèques pris en charge, reportez-vous à la section "Configurations prises en charge" à la page 292.

La sauvegarde directe nécessite que l'Agent général de supports ne se trouve pas sur le serveur d'application. En outre, l'Agent de support Resolve doit se trouver sur le serveur d'application (ou sur un autre hôte) et doit avoir accès au moteur XCopy. Pour plus d'informations sur le placement de l'Agent Resolve, reportez-vous à la section "Configurations prises en charge" à la page 292.

Les conditions pour réaliser une sauvegarde directe sont les suivantes :

- La baie de disques, le moteur XCopy, le serveur d'application et le lecteur ou la bibliothèque de bandes sont reliés au SAN.
- L'hôte Resolve et le serveur d'application sont reliés au réseau local.
- HP StorageWorks Disk Array XP (XP) utilise la configuration Business Copy (BC) avec des miroirs disposant d'un espace disque suffisant.
- Le SAN est configuré pour assurer l'accès aux périphériques source (disques) et cible (bande) depuis le moteur XCopy et depuis l'hôte sur lequel s'exécute l'Agent général de supports Data Protector. Par conséquent, le masquage des LUN et le découpage par zones du SAN doivent être paramétrés de manière à ce que :
  - L'hôte de l'Agent général de supports dispose d'un accès au moteur XCopy ;
  - L'hôte de l'Agent général de supports ait accès au lecteur ou à la bibliothèque de bandes cible ;
  - L'hôte SSEA ait accès au disque source ;
  - Le moteur XCopy ait accès au disque source ;
  - Le moteur XCopy ait accès au lecteur ou à la bibliothèque de bandes.

A propos de Resolve

Le programme Resolve est un composant propriétaire de Data Protector qui comprend la configuration native de disque de nombreux systèmes de fichiers. Resolve permet à Data Protector de procéder à la sauvegarde directe de données écrites par différents types de systèmes d'exploitation sans pour autant avoir besoin de nombreux serveurs exécutant ces systèmes d'exploitation.

Resolve analyse les informations brutes présentes sur le disque et choisit la méthode appropriée pour interpréter le système de fichiers du disque. Notez que Resolve ne lit pas les données en elles-mêmes ; il se contente de lire les informations relatives à l'emplacement du disque. Puis, il renvoie celles qui se prêtent à un transfert direct vers le moteur XCopy.

A propos de XCopy

XCopy est une norme du NCITS (National Committee for Information Technology) qui permet à deux périphériques de communiquer entre eux sans l'aide d'un ordinateur/serveur intermédiaire.

XCopy définit un ensemble de commandes SCSI qui, lorsqu'elles sont adressées à un moteur XCopy, permettent le transfert de données d'un périphérique à un autre sans l'aide d'un ordinateur/serveur intermédiaire. Les données transitent du périphérique source (en bloc ou en continu, c'est-à-dire sur disque ou sur bande) vers le périphérique cible (en bloc ou en continu) via XCopy.

Il suppose que le périphérique en mode continu (bande) est configuré et qu'il est prêt à lire/écrire les données (c'est-à-dire que le lecteur est en ligne, qu'il contient une bande et que celle-ci est correctement positionnée au point de départ de la lecture/écriture). Ainsi, le serveur de contrôle n'a plus besoin de lire les données d'un périphérique, de les enregistrer dans sa mémoire, puis de les écrire sur le périphérique de destination. Grâce à XCopy, il suffit au serveur d'envoyer les commandes XCopy au moteur XCopy, puis d'attendre les résultats.

XCopy + Resolve

Lorsque Resolve n'existait pas, il fallait un serveur doté d'un système de fichiers correspondant pour obtenir ces informations. En effet, même avec le serveur approprié, l'obtention de ces informations pouvait s'avérer difficile, car le système d'exploitation pouvait avoir converti les secteurs physiques en une vue logique avant de renvoyer les informations. Resolve supprime la nécessité de disposer de plusieurs

serveurs pour gérer de multiples systèmes de fichiers et élimine les difficultés liées aux formats d'informations spécifiques des différents systèmes de fichiers.

Flux de processus de la sauvegarde directe

La liste ci-après présente le flux de processus de la sauvegarde directe. Elle comprend les étapes fondamentales, du début à la fin, d'une opération de sauvegarde directe.

- Lecture de la spécification de sauvegarde
- Définition des éléments à sauvegarder
- Mise en attente de l'application
- Réalisation d'une copie miroir
- Redémarrage de l'application
- Résolution des blocs
- Déplacement des données vers le moteur XCopy
- Reconnexion et resynchronisation du miroir

Etapes de sauvegarde pour les fichiers de données

Les fichiers originaux à sauvegarder traversent plusieurs étapes avant de devenir des copies utilisées ultérieurement pour la récupération. Le processus de sauvegarde directe comprend (généralement) les étapes suivantes :

1. Assurer la cohérence des fichiers de données (mettre l'application en attente).
2. Lire les méta-données (attributs de fichiers) et les fichiers de groupes et les convertir en objets.
3. Assurer la stabilité des fichiers de données (utilisation de la technologie Split Mirror pour assurer la stabilité des données à un instant donné).
4. Mettre en correspondance les fichiers de données avec une liste de blocs de disque (à l'aide de la technologie Resolve).
5. Déplacer les blocs de disque vers une bande (à l'aide de la technologie XCopy).

En général, chaque étape est gérée par un agent Data Protector. Les agents sont générés par le BSM (Backup Session Manager - gestionnaire de session de sauvegarde). Toutes les erreurs qui ne peuvent pas être traitées en interne par les agents sont signalées à l'utilisateur par le BSM, puis stockées dans la base de données interne. Le BMA (Backup Media Agent - Agent de support de sauvegarde) écrit des segments de catalogue et des séparateurs entre les segments de données et de catalogue, appelés marques de fichier.

Restauration

La sauvegarde directe offre deux options de restauration :

- Si vous utilisez la baie de disques HP StorageWorks XP et que vous disposez de la fonction de restauration instantanée, vous pouvez y avoir recours pour récupérer les données. Pour obtenir une explication de la fonction de restauration instantanée, reportez-vous au *Guide de l'administrateur HP OpenView Storage Data Protector de sauvegarde avec temps d'indisponibilité nul*.
- La restauration des informations sauvegardées par sauvegarde directe peut aussi s'effectuer par le biais d'une restauration réseau Data Protector standard.

Dans les deux cas, il est important de s'assurer que le serveur d'application est capable de gérer la charge du processus de restauration. Cela n'est pas une préoccupation au niveau de la sauvegarde, car les données ne transitent pas par le serveur au cours de cette opération. Pendant la restauration, en revanche, les données exercent un impact sur le serveur.

Caractéristiques requises et éléments pris en charge

Cette section répertorie les caractéristiques requises pour une utilisation réussie de la sauvegarde directe ainsi que les systèmes de fichier et les applications pris en charge par la sauvegarde directe.

- Data Protector Le Gestionnaire de cellule de Data Protector s'exécutant sous n'importe quel système d'exploitation pris en charge.
- Agent Resolve s'exécutant sous HP-UX 11.11.
- Prise en charge de serveurs d'applications exécutant HP-UX 11.11.
- Prise en charge des LVM HP sous HP-UX 11.11.
- L'hôte XCopy, le disque source, le périphérique de destination et le moteur XCopy doivent se trouver à l'intérieur de la même zone du SAN.
- Système de fichiers pris en charge :

  — VxFS 3.1, 3.3 de Veritas
- Application prise en charge :

  — Oracle 9.i
- Volume brut pris en charge.
- Prise en charge des environnements ServiceGuard pour le serveur d'application.
- Restauration par le biais de l'interface de restauration Data Protector standard.
- Prise en charge de la restauration instantanée pour le système XP.
- Moteur XCopy dans la passerelle.

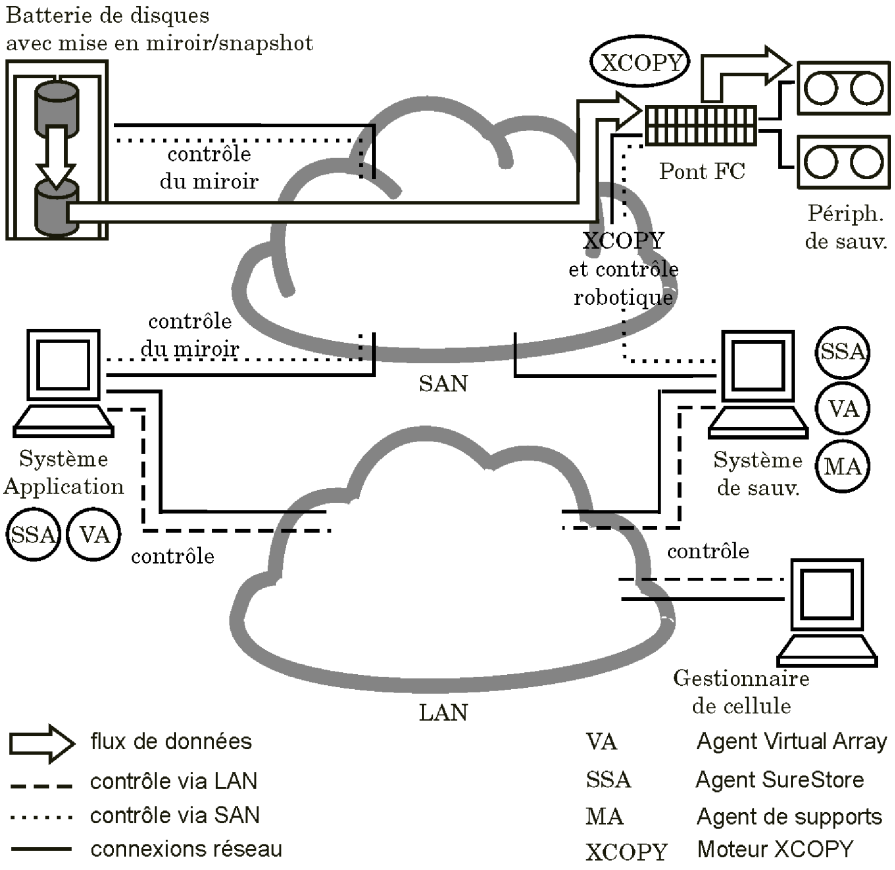
Configurations prises en charge

Trois hôtes : CM, Application, Resolve

Cette solution fait appel à trois hôtes : un premier pour le Gestionnaire de cellule, un second pour l'Agent Resolve et un troisième pour l'application. Bien que cette configuration exige l'utilisation de trois machines, elle présente néanmoins quelques avantages : l'hôte Resolve peut s'avérer moins coûteux et la charge pesant sur les ressources est partagée, évitant ainsi tout impact sur les performances de l'application.

Notez que dans cette configuration, l'hôte Gestionnaire de cellule peut exécuter *tout* système d'exploitation pris en charge par Data Protector. Les hôtes de l'application et de l'Agent Resolve doivent exécuter HP-UX 11.11.

Figure 9-2 **Configuration de base à trois hôtes**



Deux hôtes : Gestionnaire de cellule/Agent Resolve et Application

Cette solution fait appel à deux hôtes : l'un pour le Gestionnaire de cellule et l'Agent Resolve, l'autre pour l'application. Bien que cette configuration exige l'utilisation de deux machines, elle présente tout de même un avantage : la charge pesant sur les ressources est partagée, évitant ainsi tout impact sur les performances de l'application. En outre, la machine hébergeant le Gestionnaire de cellule et l'Agent Resolve peut disposer d'une capacité de calcul minimale.

Notez que dans cette configuration, les deux hôtes doivent exécuter HP-UX 11.11.

Configuration de base : hôte unique

Cette solution fait appel à un seul hôte sur lequel sont installés le Gestionnaire de cellule, l'application et l'Agent Resolve. Les trois composants s'exécutant sur une même machine, il partagent les ressources (canaux d'E/S, processeur, mémoire, etc.) pour leurs activités. Cette configuration limite le nombre d'équipements requis pour la sauvegarde directe. Cependant, les ressources étant partagées, le Gestionnaire de cellule et l'Agent général de supports peuvent avoir un impact négatif sur les performances de la base de données de l'application (la puissance de calcul requise par XCopy est négligeable).

Notez que dans cette configuration, l'hôte doit exécuter HP-UX 11.11.

10 Sauvegarde sur disques

Description du chapitre

Ce chapitre présente les concepts associés à la sauvegarde de données sur disque et les technologies permettant de la mettre en application. Il décrit également les configurations de sauvegarde disque-à-disque prises en charge par Data Protector.

Il s'organise comme suit :

"Présentation" à la page 297

"Avantages de la sauvegarde sur disque" à la page 298

"Périphériques sur disque Data Protector" à la page 300

Présentation

L'industrie requiert des méthodes de sauvegarde et de restauration de données de plus en plus rapides. En outre, il importe de plus en plus que le temps nécessaire à la sauvegarde et à la restauration des données soit réduit au minimum afin de ne pas interrompre le fonctionnement quotidien des applications de l'entreprise.

Au cours d'un jour ouvrable, nombre d'applications et de bases de données ne cessent d'apporter de petites modifications aux fichiers existants ou de générer une grande quantité de fichiers nouveaux contenant des données stratégiques. Ces fichiers doivent être sauvegardés immédiatement pour que les données qu'ils contiennent ne soient pas perdues. Cette condition implique l'utilisation d'un support rapide pouvant stocker des volumes de données importants et fonctionnant de manière ininterrompue.

Le prix des supports de stockage sur disque est devenu plus abordable ces dernières années. Dans le même temps, la capacité de stockage s'est accrue. En conséquence, des disques simples et des baies de disques à faible coût et hautement performants sont désormais disponibles pour le stockage de données.

La sauvegarde sur disque (également appelée sauvegarde disque à disque) prend une importance croissante. Auparavant, le stockage sur bande était la méthode de prédilection pour la sauvegarde et la restauration en raison de son coût et de sa capacité à satisfaire aux exigences de récupération après sinistre. Aujourd'hui, un nombre croissant d'entreprises complètent leurs solutions de sauvegarde sur bande par des solutions de sauvegarde sur disque plus rapides. Les données sont ainsi sauvegardées et récupérées plus rapidement.

Avantages de la sauvegarde sur disque

Dans bon nombre de cas, il n'est pas avantageux d'utiliser des périphériques sur disque pour effectuer des sauvegardes. Les périphériques sur disque sont en fait des fichiers spécifiques dans des répertoires spécifiés sur lesquels vous pouvez stocker des données au lieu ou en plus de les stocker sur bande. La liste suivante présente certaines situations dans lesquelles les périphériques sur disque sont particulièrement utiles :

- De nombreuses applications et bases de données génèrent ou modifient en permanence un grand nombre de fichiers contenant des données stratégiques. Dans ces situations, il est nécessaire de sauvegarder régulièrement les fichiers concernés afin de garantir une restauration sans perte de données.

  Dans ces environnements, les périphériques à bande doivent fonctionner généralement en mode marche/arrêt car ils ne reçoivent pas un flux continuel de données. Le périphérique à bande peut alors limiter l'accès aux fichiers concernés. En outre, la durée de vie du périphérique de sauvegarde peut être considérablement réduite.

  Les sauvegardes peuvent également être réalisées sur un périphérique sur disque, ce qui permet de dépasser les limites décrites. Elle peut faire office de solution de sauvegarde à court terme. Si une solution de sauvegarde à long terme est requise, les données contenues dans les périphériques sur disque peuvent être déplacées régulièrement sur une bande afin de libérer l'espace disque. Ce processus est appelé **sauvegarde de disque en plusieurs étapes**.

- Dans les environnements caractérisés par des lecteurs de disque rapides et très performants et des lecteurs de bande lents, vous pouvez réduire la fenêtre de sauvegarde en effectuant tout d'abord une sauvegarde sur les périphériques sur disque et en déplaçant ensuite les données sur une bande.

- Les périphériques sur disque permettent de restaurer rapidement des données sauvegardées récemment. Par exemple, les données de sauvegarde peuvent être conservées sur un périphérique sur disque pendant 24 heures pour permettre une restauration rapide et pratique.

- Le mécanisme d'un périphérique sur disque est plus rapide que celui d'une bande. Lors de l'utilisation d'un périphérique sur disque, il n'est pas nécessaire de monter et de démonter la bande. Lors de la sauvegarde ou de la restauration d'un petit volume de données, un périphérique sur disque est plus rapide car son temps d'initialisation est bien moins important que celui d'un lecteur de bande. Dans le cas d'un périphérique sur disque, il n'est pas nécessaire de charger ou de décharger les supports, des tâches fastidieuses dans le cas d'une sauvegarde ou d'une restauration de petite taille. Les avantages de l'utilisation d'un périphérique sur disque apparaissent encore plus évidents lorsqu'on effectue une restauration à partir d'une sauvegarde incrémentale.
- La probabilité de rencontrer des problèmes au niveau des supports, tels que des bandes défectueuses ou un montage incorrect de la bande, est quasiment nulle. La disponibilité des configurations de disque RAID garantit la protection des données en cas de dysfonctionnement d'un disque.
- Les frais généraux sont réduits car il n'est pas nécessaire de manipuler les bandes.
- En règle générale, le stockage sur disque devient de moins en moins onéreux, même comparé au stockage sur bande.

Périphériques sur disque Data Protector

Data Protector est doté des périphériques sur disque suivant :

- Périphérique de fichiers autonome
- Périphérique de bibliothèque de stockage de fichiers
- Périphérique de bibliothèque de fichiers

Périphérique de fichiers autonome

Le périphérique de fichiers autonome est le plus simple des systèmes de sauvegarde sur disque. Il se compose d'un simple logement dans lequel les données peuvent être sauvegardées. Une fois configurées, ses propriétés sont immuables. Le périphérique de fichiers possède une capacité maximale de 2 To, si cette taille de fichier est prise en charge par le système d'exploitation sur lequel le périphérique fonctionne.

Périphérique de bibliothèque de stockage de fichiers

Le périphérique de bibliothèque de stockage de fichiers est une version spéciale du périphérique de bibliothèque de stockage Data Protector. Le périphérique de bibliothèque de stockage peut être configuré pour sauvegarder des supports optiques ou des fichiers. Le périphérique de bibliothèque de stockage utilisé pour sauvegarder des fichiers est appelé périphérique de bibliothèque de stockage de fichiers. Le type de supports sauvegardé par le périphérique de bibliothèque de stockage est spécifié pendant la configuration du périphérique.

Le périphérique de bibliothèque de stockage de fichiers se compose de plusieurs logements dans lesquels vous pouvez sauvegarder des données. La configuration est un processus en deux phases : on crée d'abord un périphérique de bibliothèque de stockage de fichiers, puis on configure un ou plusieurs lecteurs pour ce périphérique de bibliothèque de stockage. Une fois le périphérique configuré, il est possible de modifier ses propriétés. Chaque logement du périphérique de bibliothèque de stockage de fichiers possède une capacité maximale de 2 To. La capacité maximale du périphérique est égale à :

```
Nombre de logements X 2 To
```

Périphérique de bibliothèque de fichiers

Le périphérique de bibliothèque de fichiers est le plus perfectionné des systèmes de sauvegarde sur disque. Elle dispose de multiples logements appelés **dépôts de fichier** dans lesquels vous pouvez sauvegarder des données. La configuration du périphérique de bibliothèque de fichiers s'effectue en une seule étape. Il est possible de modifier les propriétés du

périphérique de bibliothèque de fichiers à tout moment. La capacité maximale de la bibliothèque est identique à la capacité maximale du système de fichiers sur lequel elle réside. Chaque dépôt de fichier possède une capacité maximale de 2 To. Les dépôts de fichier sont créés automatiquement selon les besoins.

Le périphérique de bibliothèque de fichiers utilise une gestion intelligente de l'espace disque. Il anticipe les problèmes potentiels liés à l'enregistrement des données. Un message d'avertissement est inscrit dans le journal des événements si l'espace disque disponible approche le minimum configuré requis pour que le périphérique fonctionne. Cela vous permet de libérer de l'espace disque à temps pour permettre au périphérique de continuer à enregistrer des données. Si l'ensemble de l'espace alloué au périphérique de bibliothèque de fichiers vient à être utilisé, un message d'avertissement apparaît à l'écran, avec des instructions permettant de résoudre le problème.

Le périphérique de bibliothèque de fichiers crée automatiquement de nouveaux dépôts de fichier si une sauvegarde particulière requiert plus d'espace que n'en contient un seul dépôt de fichiers.

Périphérique de sauvegarde sur disque recommandé

Hewlett-Packard recommande l'utilisation du périphérique de bibliothèque de fichiers en tant que périphérique favori de sauvegarde sur disque. Le périphérique de bibliothèque de fichiers est le plus flexible et le plus intelligent des périphériques de sauvegarde sur disque. Il est possible de la reconfigurer à tout moment pendant son utilisation et elle est capable de gérer l'espace disque de manière plus perfectionnée que les autres périphériques de sauvegarde sur disque. Les fonctionnalités du périphérique de bibliothèque de fichiers sont décrites en détail dans le *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Format de données

Le format de données des périphériques sur disque s'appuie sur le format de données pour bandes. Data Protector convertit au format de bande les données à sauvegarder avant de les écrire sur le périphérique sur disque.

Configuration

Il est possible de définir les propriétés de tous les périphériques sur disque pendant la configuration initiale des périphériques et après l'utilisation de ces derniers. Le degré de modification pouvant être apporté aux propriétés de chaque périphérique varie en fonction du périphérique.

Sauvegarde sur un périphérique sur disque

Il est possible d'effectuer une sauvegarde sur un périphérique sur disque en créant une spécification de sauvegarde Data Protector normale.

11 Concepts Split Mirror

Description du chapitre

Le présent chapitre décrit le concept de la sauvegarde Split Mirror ainsi que les configurations prises en charge par HP.

Il s'organise comme suit :

"Présentation" à la page 305

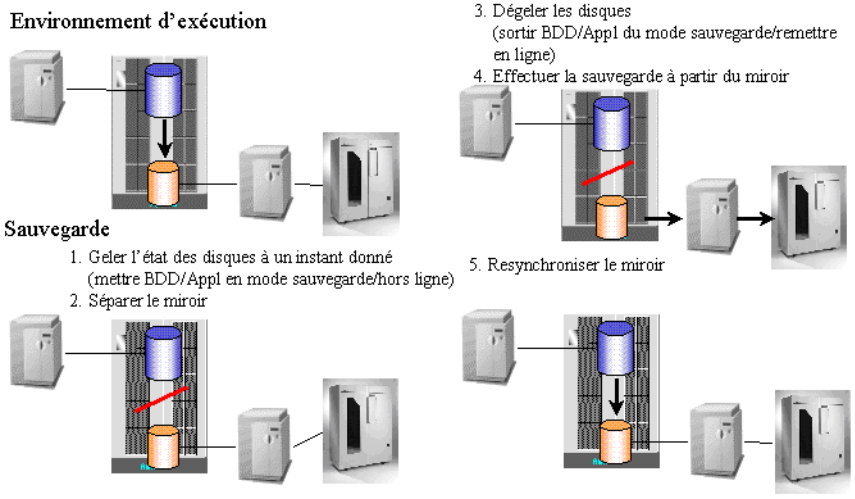
"Configurations prises en charge" à la page 309

Présentation

Aujourd'hui, les configurations de stockage modernes haute disponibilité (HA, pour High Availability) reflètent les nouvelles exigences en termes de sauvegarde. La configuration est l'une des nombreuses variations possibles de structures de miroir simple ou multiple.

L'approche générale consiste à utiliser une **réplique** (copie miroir) pour procéder à la sauvegarde, tandis que les **volumes source** continuent à servir l'application. Reportez-vous à la figure 11-1.

Figure 11-1 **Concept de la sauvegarde Split Mirror**



Les **volumes cible** de la réplique sont généralement connectés à un client distinct, auquel sont également reliés des périphériques à bande pour les sauvegardes locales. Des technologies de mise en miroir de matériel telles que HP StorageWorks Disk Array XP ou EMC Symmetrix sont généralement utilisées pour créer une réplique telle que :

- HP StorageWorks ContinuousAccess XP ou
- HP StorageWorks BusinessCopy XP

L'application est disponible pratiquement en permanence, excepté pendant une courte période (qui peut aller de plusieurs secondes à quelques minutes). Au cours de cette période, le système assure la

cohérence des données sur le disque et réalise la séparation effective des miroirs. Les données doivent être cohérentes pour que l'application puisse les utiliser après une restauration. En principe, la réplique miroir n'est pas créée au moment de la sauvegarde ; elle est déjà disponible et synchronisée à ce stade afin que l'application bénéficie d'une disponibilité élevée. La sauvegarde et la resynchronisation de la réplique n'affectent pas les performances de l'application, car ces opérations s'effectuent en parallèle, sur un équipement séparé.

Le client de l'application et celui de la sauvegarde étant différents (dans la plupart des cas), toutes les informations mises en cache (cache de la base de données, cache du système de fichiers) du client doivent être transférées vers le disque avant que le miroir de la sauvegarde ne soit séparé. Pour cela, effectuez l'une des opérations suivantes :

- Configurez les bases de données en mode sauvegarde.
- Mettez les bases de données hors ligne.
- Démontez un point de montage.

Une réplique ne sera cohérente que si vous effectuez ces opérations *au préalable*. Cependant, si la base de données s'exécute sur un système de fichiers ou sur un rawdisk, il n'est pas nécessaire de démonter ce système de fichiers ou rawdisk, car la base de données s'assure que les données sont effectivement écrites sur le disque et non dans le cache du système de fichiers.

Dans le cas d'une sauvegarde de base de données en ligne, une réplique seule ne peut pas être restaurée. Les journaux d'archive du client d'application sont également requis. Vous pouvez démarrer une sauvegarde du journal d'archive juste après la séparation, lorsque la base de données n'est plus en mode sauvegarde.

L'utilisation combinée d'une réplique et de la technologie HP StorageWorks ContinuousAccess XP pour réaliser une sauvegarde affecte la haute disponibilité de stockage pendant la durée de cette sauvegarde. Si vous disposez de miroirs supplémentaires, vous pouvez conserver la haute disponibilité de stockage tout en utilisant la même démarche de sauvegarde.

Le client de sauvegarde peut être le client central de plusieurs clients d'application exécutant différentes applications. Dans ce cas, le client de sauvegarde doit s'exécuter sur le même système d'exploitation que le client d'application, afin d'accéder aux ressources mises en miroir de façon native.

Le client de sauvegarde doit pouvoir effectuer les sauvegardes dans un temps raisonnable. Bien qu'une sauvegarde puisse durer, en théorie, près de 24 heures, vous devez également prendre en compte le temps de restauration. Il est donc recommandé de prévoir un client de sauvegarde capable d'effectuer les sauvegardes en deux à quatre heures, et de réaliser les restaurations au moyen du client d'application.

Avec cette approche, la majeure partie du transfert des données s'effectue via le client de sauvegarde et son accès à la réplique. La connexion réseau entre le client de sauvegarde et le client d'application sert uniquement à coordonner les processus impliqués dans la sauvegarde. De plus, des processus s'exécutent sur chaque client afin d'automatiser la séparation.

Restauration instantanée

Data Protector assure une restauration instantanée reposant sur la technologie Split Mirror. La solution est basée sur des solutions de sauvegarde avec temps d'indisponibilité nul telles que l'intégration HP StorageWorks Disk Array XP, laquelle emploie la technologie Split Mirror.

Pendant une session de sauvegarde Split Mirror, une réplique est utilisée pour le transfert des données sur un support de sauvegarde (bande). Après la sauvegarde, vous pouvez supprimer la réplique et préparer deux disques pour la prochaine session de sauvegarde par resynchronisation, ou bien conserver la réplique en vue d'une restauration instantanée. Plusieurs répliques peuvent exister simultanément. Grâce à HP StorageWorks Disk Array XP, vous pouvez par exemple réaliser jusqu'à trois répliques, chacune d'elles pouvant être copiée deux fois si vous utilisez le traitement en cascade.

Pendant la restauration instantanée, les données présentes sur la réplique spécifiée (inchangée à des fins de restauration instantanée) sont synchronisées avec les volumes sources du client d'application et non restaurées depuis un support de sauvegarde.

Data Protector n'utilise que les trois premières répliques ; en effet, les copies miroir secondaires ne permettent pas d'assurer une resynchronisation rapide, laquelle est essentielle pour réduire au minimum le temps de restauration. La restauration instantanée n'est possible qu'avec la configuration HP StorageWorks BusinessCopy XP (configurations miroir local - hôte double et miroir local - hôte simple).

Sauvegarde sur bande avec temps d'indisponibilité nul et ZDB sur disque + bande

Lors d'une session de sauvegarde sur bande ou sur disque+bande avec temps d'indisponibilité nul, une réplique des données d'application est écrite en flux continu sur un périphérique de bande connecté à un système de sauvegarde séparé, à l'aide de l'Agent de disque et de l'Agent général de supports Data Protector, et ce avec une incidence minimale sur le système d'application. Une fois la sauvegarde terminée, la réplique est :

- Supprimée - sauvegarde sur bande avec temps d'indisponibilité nul
- Conservée en vue d'une restauration instantanée - ZDB sur disque + bande

Sauvegarde sur disque avec temps d'indisponibilité nul

Pendant une session de sauvegarde sur disque avec temps d'indisponibilité nul, les données originales sont déplacées vers un support de sauvegarde (bande) à partir de la réplique. Les répliques (trois au maximum) peuvent avoir diverses utilisations, notamment le traitement de données hors ligne ou la restauration instantanée ; cette dernière n'est possible que si la configuration StorageWorks BusinessCopy XP est utilisée. La restauration d'objets à partir d'une session de sauvegarde sur disque avec temps d'indisponibilité nul n'est possible qu'avec la fonctionnalité de restauration instantanée.

Rotation du jeu de répliques

Plusieurs répliques peuvent exister simultanément. HP StorageWorks Disk Array XP permet de réaliser jusqu'à trois répliques, chacune d'elles pouvant être copiée deux fois si vous utilisez le traitement en cascade. Data Protector ne peut utiliser que les disques des trois premières répliques (les **miroirs de premier niveau** ou **MU**) pour les opérations de sauvegarde et de restauration instantanée. Les six copies supplémentaires (miroirs en cascade) ne sont pas prises en charge.

Lors de la configuration d'une spécification de sauvegarde avec temps d'indisponibilité nul pour un volume source (LDEV) avec des miroirs de premier niveau configurés ou lors de la restauration vers ce volume source, il est possible, en utilisant Data Protector, de définir un **jeu de répliques** à partir duquel cette intégration sélectionne une réplique pour la session en cours.

Clients de sauvegarde et clusters

Le client de sauvegarde ne doit pas être utilisé comme serveur de basculement pour le client d'application. Il est recommandé d'installer les services d'application et de sauvegarde sur des clusters séparés.

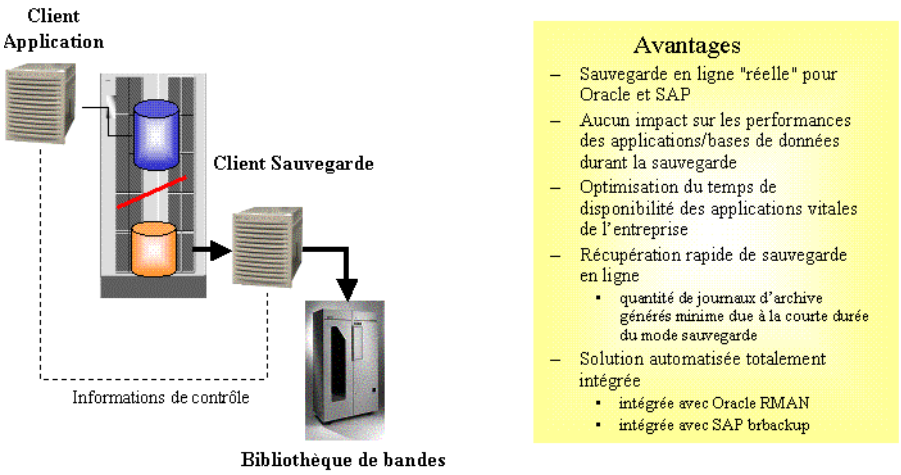
Configurations prises en charge

Miroir local - hôte double

Cette solution utilise une fonction de mise en miroir locale (Business Copy XP, par exemple). Les deux disques se trouvent dans la même baie de disques, ce qui signifie que l'infrastructure d'E/S du système RAID est partagée entre le client d'application (ou hôte) et le client de sauvegarde.

Le client d'application et le client de sauvegarde étant deux systèmes physiquement différents, ils peuvent utiliser leurs propres ressources (canaux d'E/S, unités centrales, mémoire, etc.) pour réaliser leurs activités spécifiques, par exemple effectuer une sauvegarde, sans incidence sur le fonctionnement de l'autre. Ainsi, les performances de la sauvegarde n'influent pas sur celles de la base de données.

Figure 11-2 **Miroir local - hôte double (sauvegarde avec performance optimale et temps d'indisponibilité nul)**



L'intégration de sauvegarde Split Mirror Data Protector permet le traitement automatique de l'état du miroir ainsi qu'une intégration avec des applications telles que SAP R/3 et Oracle (afin d'assurer la cohérence des données et de signaler les sauvegardes à l'application / la base de données). Pour assurer une opération sécurisée et utiliser les outils

d'application natifs pour la restauration (`sapdba`, par exemple), il faut que la sauvegarde soit prise en compte au préalable par l'application / la base de données. L'impact d'une sauvegarde sur l'application est réduit au temps nécessaire pour effectuer une séparation du miroir et pour mettre la base de données dans un mode cohérent permettant la séparation, puis lui faire quitter ce mode.

Cette configuration permet de réaliser en peu de temps une sauvegarde hors ligne à partir d'une base de données très volumineuse, ainsi qu'une sauvegarde en ligne générant très peu de journaux d'archive, la durée pendant laquelle la base de données reste en mode sauvegarde étant réduite au minimum.

Le fait de générer peu de journaux d'archive réduit l'espace nécessaire pour ce type de fichiers et accélère le processus de récupération de la base de données. Après la restauration d'une base de données en ligne, il est nécessaire d'effectuer une récupération afin que les données de la base redeviennent cohérentes. Tous les journaux d'archive créés au cours de la sauvegarde doivent être utilisés. Dans le cas d'une sauvegarde Split Mirror, seuls les fichiers journaux d'archive créés au cours de la séparation sont appliqués.

Miroir local - hôte simple

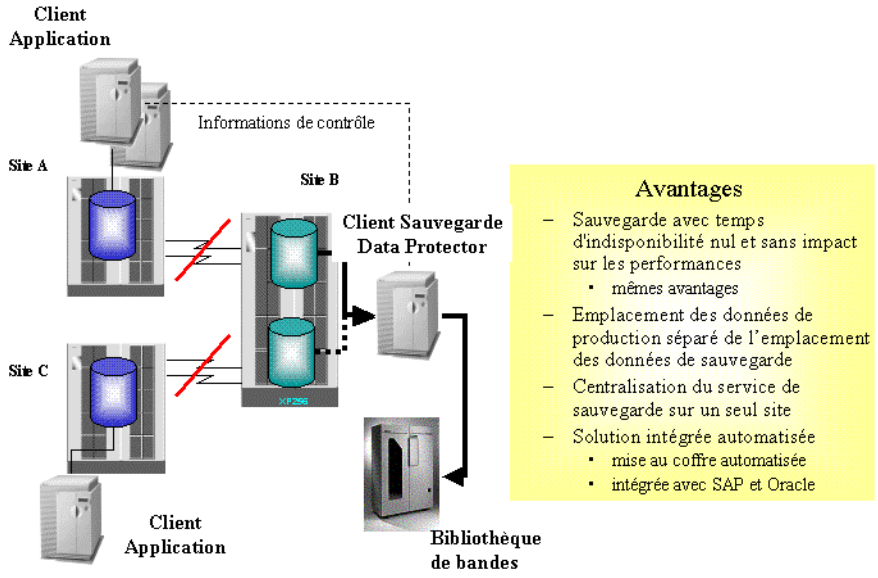
Dans les cas où aucun serveur de sauvegarde dédié n'est disponible, les deux fonctions (application et sauvegarde) sont effectuées sur le même client (ou hôte). Les sauvegardes hors ligne des applications de messagerie, par exemple, peuvent réduire le temps d'indisponibilité de l'application de quelques heures à quelques minutes.

Dans ce type de configuration, seules les sauvegardes d'**image disque** (raw disk) et du **système de fichiers** sont prises en charge. Les sauvegardes de base de données et d'application, telles qu'Oracle et SAP R/3, ne peuvent pas être prises en charge car la base de données doit être montée sur le serveur de sauvegarde ; or, il n'est pas possible d'effectuer cette opération sur le serveur sur lequel la base de données est déjà montée.

Miroir distant

La technologie de miroir distant, Continuous Access XP par exemple, améliore les configurations citées plus haut car les processus de sauvegarde et d'application utilisent différentes baies de disques à différents endroits.

Figure 11-3 **Split Mirror - miroir distant (sauvegarde distante indépendante du réseau local - données haute disponibilité)**



Le miroir distant transfère les données vers un site physiquement séparé. Celles-ci peuvent alors être sauvegardées sur des bandes disponibles en local. Cette opération permet de séparer les données de production des données de sauvegarde et par conséquent, d'éliminer le risque de dommages à ces deux types de données en même temps en cas d'incendie ou d'un autre sinistre.

Au cours d'une sauvegarde, la synchronisation des miroirs ne requiert aucune ressource réseau. Bien que les données ne soient pas transférées via le réseau, Data Protector a néanmoins besoin de la communication entre le Gestionnaire de cellule et ses clients.

Cette solution vous permet de centraliser un service de sauvegarde en mettant en miroir les données d'application provenant de plusieurs sites de production (A et C dans ce cas) dans un lieu unique ou une baie de disques centralisée. Ainsi, votre investissement dans un service de sauvegarde (serveur et bibliothèque de bandes) peut être consolidé et combiné avec la haute disponibilité d'une configuration à miroir distant.

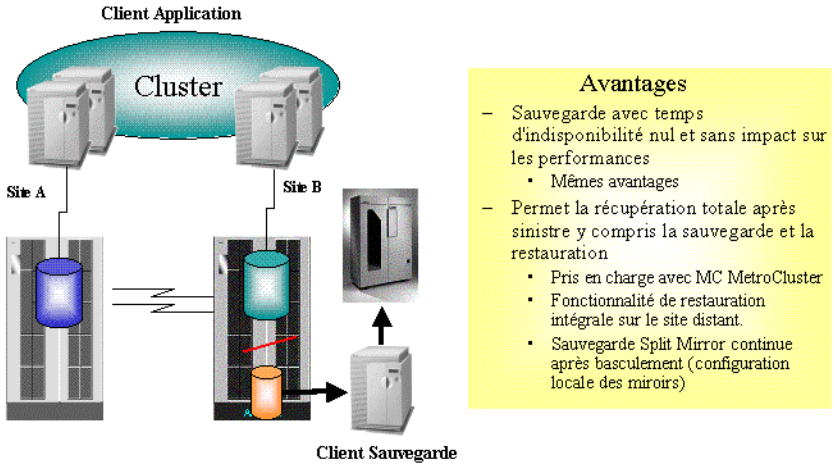
Le site distant ne peut pas être utilisé comme site de récupération après sinistre automatique pendant que la sauvegarde s'effectue, car le lien entre les deux sites est alors rompu (et les deux disques ne sont pas synchronisés). Ceci signifie qu'en cas de défaillance du site A, le site B ne peut pas prendre le relais automatiquement (ce qu'il ferait normalement) pendant x heures (x correspondant au temps nécessaire pour que les données soient copiées sur la bande). Ce problème concerne également les mises en miroir locales. Toutefois, cela pose surtout des problèmes pour la solution distante, car le concept d'un site distant de récupération après sinistre distante faisant appel aux miroirs de matériel est largement répandu sur le marché.

Combinaison de miroirs local et distant

Si le client a besoin de disposer en permanence d'un site de récupération disponible (fourni, par exemple, par un MetroCluster) et d'effectuer des sauvegardes avec un temps d'indisponibilité nul, il est possible de combiner le miroir distant avec le miroir local.

Cette solution présente tous les avantages du Split Mirror et permet d'effectuer une récupération complète vers le site distant. Dans cet exemple, le miroir distant est maintenu en permanence et le lien local n'est séparé que pour effectuer des sauvegardes. Le cluster peut donc basculer à tout moment sur le site distant (site B).

Figure 11-4 **Combinaison de miroirs local et distant (récupération après sinistre intégrée à la sauvegarde : service haute disponibilité - HP UX uniquement)**



Pour que la fonction de basculement soit indépendante de l'opération de sauvegarde, le client de sauvegarde doit être un client supplémentaire séparé et se trouver en dehors du cluster. Si une solution MetroCluster est mise en place, le client d'arbitrage de cluster peut être le client de sauvegarde.

Autres configurations

Il existe de nombreuses autres configurations Split Mirror qui fournissent des avantages spécifiques ou répondent aux besoins de certains utilisateurs. Toutefois, chacune est associée à un modèle de comportement spécifique représentant des exigences particulières auxquelles les fonctions de contrôle doivent obéir afin de garantir la sauvegarde et la récupération. Il est donc important de vérifier quelles configurations sont prises en charge et de les spécifier.

Toutes les configurations décrites précédemment sont prises en charge par HP. Pour obtenir une liste récente des configurations prises en charge, consultez l'adresse suivante : http://www.openview.hp.com/products/datapro/spec_0001.html.

Si une configuration dans laquelle vous souhaitez sauvegarder des données n'est pas répertoriée dans la liste, cela ne signifie pas que l'opération ne peut pas être prise en charge. Contactez votre représentant HP local ou votre consultant HP pour connaître les autres configurations prises en charge.

12 Concepts de snapshot

Description du chapitre

Le présent chapitre décrit le concept de sauvegarde de snapshot, ainsi que les configurations prises en charge par HP.

Il s'organise comme suit :

"Présentation" à la page 317

"Configurations prises en charge" à la page 324

Présentation

Pour répondre à la demande croissante en configurations de stockage haute disponibilité, de nouvelles technologies de sauvegarde avec temps d'indisponibilité nul ont été mises au point. D'autre part, les progrès en matière de technologie de virtualisation de stockage procurent aujourd'hui une alternative à la technologie Split Mirror conventionnelle.

La solution de sauvegarde avec temps d'indisponibilité nul Data Protector associe différentes technologies de baies de disques aux derniers développements en matière de technologie de "snapshot" (image figée) pour créer des snapshots de données d'applications ou de bases de données enregistrées sur une baie de disques. Ces snapshots peuvent ensuite être conservés sur une baie de disques sous forme de copies ponctuelles des données d'origine à des fins de **restauration instantanée**, ou peuvent être utilisées pour créer des sauvegardes sur bande avec temps d'indisponibilité nul sur un système de sauvegarde. Les processus impliqués ont peu d'impact sur le serveur d'applications, offrant ainsi une solution réelle en termes de sauvegarde avec temps d'indisponibilité nul.

Virtualisation du stockage

Le terme "virtualisation du stockage" fait référence à la technologie qui permet de séparer la représentation logique du stockage des composants de stockage physiques réels. Elle implique la création de volumes logiques en dehors d'un pool de disques physiques résidant sur une baie de disques. Un volume logique est limité au cadre du pool mais peut s'étendre sur un nombre quelconque de disques physiques au niveau de la baie de disques. Un ou plusieurs systèmes hôtes peuvent utiliser les volumes logiques. Il est impossible de gérer précisément l'allocation de volumes logiques sur des disques physiques ; différentes options de protection permettent toutefois de définir une orientation.

RAID

La technologie RAID (pour Redundant Array of Inexpensive Disks, ou baie de disques durs redondants économiques) permet de définir le mode de distribution des données sur les disques physiques au niveau d'une baie de disques. Il existe différents niveaux RAID, correspondant à différents niveaux de redondance et de sécurité de données, de taux de

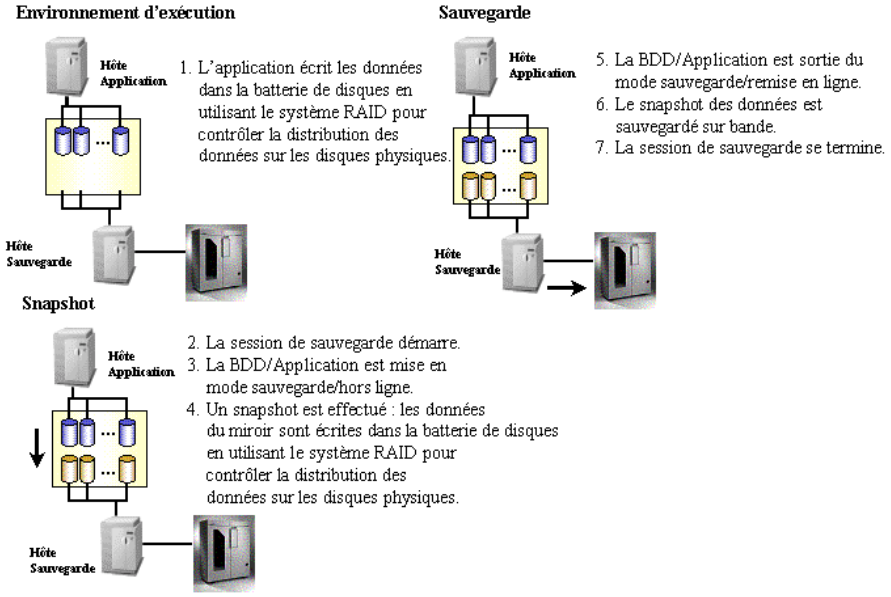
transfert et de temps d'accès. Par exemple, le niveau RAID0 n'implique aucune duplication des données, RAID1 implique la duplication de toutes les données et RAID5 implique la protection des données par parité.

Les fonctions de snapshot Data Protector intégrées ont été conçues pour être utilisées avec des baies de disques prenant en charge les technologies de snapshot, telles que HP StorageWorks Virtual Array et HP StorageWorks Enterprise Virtual Array.

Concepts de snapshot

Dans une configuration de base standard utilisant la technologie de snapshot, une baie de disques individuelle peut être connectée à des systèmes d'application et de sauvegarde séparés. La baie de disques peut être utilisée comme périphérique de stockage par le système d'application et le système de sauvegarde, et les volumes logiques peuvent être montés sur l'un ou l'autre. Lorsque ce schéma est appliqué, le système d'application utilise les volumes logiques de la baie de disques pour le stockage de ses données en période de fonctionnement normal. Les volumes logiques sur lesquels sont stockées les données du système d'application pour les besoins des fonctions de snapshot Data Protector intégrées sont également appelés **volumes source**. Lorsqu'une sauvegarde de snapshot est réalisée, les données d'application résidant au niveau des volumes source sont dupliquées et écrites sur d'autres volumes logiques de la même baie de disques, également appelés **volumes cible**. Les données ainsi dupliquées sont également appelées données snapshot. Elles correspondent à des copies ponctuelles instantanées d'un système de fichiers ou d'un volume donné. L'ensemble des volumes cible ainsi créés est également appelé **réplique**. Une fois la réplique des données snapshot créée, il est possible d'apporter des modifications aux données d'origine sans perturber le déroulement de l'opération de sauvegarde.

Figure 12-1 Sauvegarde de snapshot



Le client de sauvegarde est configuré comme client Data Protector auquel des périphériques à bande sont connectés en vue de réaliser des sauvegardes en local.

Lorsqu'une session de sauvegarde commence, le client d'application passe en mode sauvegarde tandis que le système prépare le client de sauvegarde en vue de la procédure de sauvegarde ; un snapshot des données d'application est généré.

Lorsque le client de sauvegarde est prêt et que la réplique des données snapshot est créée, l'application revient en mode de fonctionnement normal.

Le niveau de disponibilité de l'application reste pratiquement inchangé pendant que le client d'application est en mode sauvegarde (dans certains cas, l'application peut être arrêtée pendant un bref laps de temps).

Si l'on a spécifié une sauvegarde sur bande avec temps d'indisponibilité nul, les données snapshot sont ensuite écrites en flux continu sur des supports à bande au niveau du client de sauvegarde. Cette opération ne perturbe pas le fonctionnement du client d'application.

Les clients d'application et de sauvegarde étant généralement distincts, il est impératif de transférer toutes les informations mises en cache (caches de la base de données et du système de fichiers) du client d'application vers la batterie avant la création du snapshot. Pour cela, effectuez l'une des opérations suivantes :

- Configurez les bases de données en mode sauvegarde.
- Mettez les bases de données hors ligne.
- Démontez un point de montage.

Dans le cas d'une sauvegarde de base de données en ligne, les données snapshot ne permettent pas à elles seules de procéder à la restauration. Les journaux d'archive du client d'application sont également requis. Vous pouvez utiliser la procédure de sauvegarde standard Data Protector pour effectuer une sauvegarde de journaux d'archive immédiatement après la création des snapshots, lorsque que la base de données n'est plus en mode sauvegarde.

Les données snapshot correspondant aux données d'application peuvent être créées au moyen de technologies de baies de disques virtuelles, telles que :

- HP StorageWorks Business Copy Virtual Array
- HP StorageWorks Enterprise Virtual Array

Types de sauvegardes de snapshot

Les types de sauvegardes de snapshot suivants sont disponibles dans le cadre des fonctions de snapshot Data Protector intégrées :

- Sauvegarde sur bande avec temps d'indisponibilité nul
- Sauvegarde sur disque avec temps d'indisponibilité nul
- ZDB sur disque + bande

Sauvegarde sur bande avec temps d'indisponibilité nul et ZDB sur disque + bande

Lors d'une session de sauvegarde sur bande ou sur disque+bande avec temps d'indisponibilité nul, un snapshot des données d'application réalisé à un instant donné est écrit en flux continu sur un périphérique à bande connecté à un système de sauvegarde séparé, à l'aide de l'Agent de disque et de l'Agent général de supports Data Protector, et ce avec une incidence minimale sur le système d'application. Une fois la sauvegarde terminée, les données snapshot sont :

- Supprimées - sauvegarde sur bande avec temps d'indisponibilité nul
- Conservées en vue d'une restauration instantanée - ZDB sur disque + bande

Sauvegarde sur disque avec temps d'indisponibilité nul

La technologie employée lors d'une session de sauvegarde sur disque avec temps d'indisponibilité nul est identique à celle utilisée lors d'une sauvegarde sur bande ou d'une ZDB sur disque + bande ; toutefois, les données snapshot ne sont pas écrites en flux continu sur un support de sauvegarde (périphérique à bande) à partir de la copie snapshot mais sont conservées sur une baie de disques. Elle peut être utilisée pour la restauration instantanée. La session se termine dès que les données snapshot sont créées.

Restauration instantanée

Pendant les sessions de sauvegarde de snapshot, plusieurs copies snapshot des données peuvent être produites et conservées sur une baie de disques, chaque copie étant effectuée à un instant donné dans sa propre réplique. Les copies snapshot conservées peuvent ensuite être utilisées pour la restauration instantanée, le traitement de données hors ligne ou à d'autres fins. Seules les copies ponctuelles générées lors de sessions de sauvegarde sur disque ou sur disque+bande avec temps d'indisponibilité nul peuvent être restaurées au moyen de la fonctionnalité de restauration instantanée.

En cas de restauration instantanée, la copie ponctuelle d'une réplique sélectionnée est restaurée sur une baie de disques dans l'état dans lequel elle se trouvait au moment où les données snapshot ont été générées. Aucun transfert de données à partir d'un support de bande n'étant requis dans le cadre de cette procédure, la durée de restauration globale est considérablement réduite.

Les journaux d'archive d'application ne sont pas compris dans une sauvegarde de snapshot ; par conséquent, il est nécessaire de les récupérer à partir de supports à bande pour les restaurer et les utiliser.

Jeu de répliques et rotation d'un jeu de répliques

Le nombre maximal de répliques pouvant être conservées simultanément sur une baie de disques dépend de la baie de disques utilisée. Les répliques conservées sur une baie de disques dans le cadre d'une même spécification de sauvegarde constituent le **jeu de répliques**

de cette spécification de sauvegarde. Le jeu de répliques dépend du nombre maximal de répliques pouvant être conservées sur une baie de disques dans le cadre d'une spécification de sauvegarde donnée. Lorsque cette limite maximale est atteinte lors d'une session de sauvegarde de snapshot, les données snapshot de la plus ancienne réplique contenue dans le jeu de répliques sont écrasées. Tant que la limite n'est pas atteinte, le système crée une nouvelle réplique. Ces deux opérations s'inscrivent dans le cadre de la procédure de **rotation du jeu de répliques**.

Types de snapshots

Suivant la baie de disques utilisée, différents types de snapshots peuvent être créés lors d'une session de sauvegarde snapshot Data Protector. Les types de sauvegarde suivants sont utilisés dans le cadre des fonctions de snapshot Data Protector intégrées :

- Snapshots de type copie par écriture (copy-on-write) avec préallocation d'espace disque.
- Snapshots de type copie par écriture (copy-on-write) sans préallocation d'espace disque.
- Snapclones.

Snapshots avec préallocation d'espace disque

La création de snapshots de type copie par écriture (copy-on-write) avec préallocation d'espace disque requiert la même quantité d'espace disque que celle allouée au volume source. Les données ne sont écrites sur cet espace réservé qu'en cas de besoin. Les modifications apportées aux données du volume source sont répercutées sur les données snapshot du volume cible.

Dans le cadre du système de snapshot, seules les modifications apportées aux données d'origine (en constante évolution) par rapport à un état donné sont mises en cache; c'est la raison pour laquelle les snapshots de type copie par écriture (copy-on-write) avec préallocation d'espace disque sont tributaires de leurs volumes source : si les données des volumes source sont perdues, les snapshots associés sont inutilisables.

Snapshots sans préallocation d'espace disque

Les snapshots de type copie par écriture (copy-on-write) sans préallocation d'espace disque correspondent également à une copie ponctuelle des données d'origine mais ne requièrent pas de préallocation d'espace disque. L'espace disque est alloué à la demande de façon dynamique. Lorsque des modifications sont apportées aux données du

volume source, le système utilise l'espace disponible sur une baie de disques pour la création du snapshot. Les snapshots de type copie par écriture (copy-on-write) sans préallocation d'espace disque ne sont utiles qu'à court terme. Notez que la taille de ces snapshots augmente de façon dynamique : si l'on ne supprime pas régulièrement ces snapshots, l'espace de stockage risque d'être saturé.

Le principal avantage des snapshots de type copie par écriture (copy-on-write) sans préallocation d'espace disque, par rapport à ceux avec préallocation d'espace disque, tient au fait qu'ils permettent de réduire les coûts de façon significative. Si les snapshots sont supprimés régulièrement, cette technologie requiert beaucoup moins d'espace de stockage pour la duplication que la technologie de snapshot standard.

Dans le cadre du système de snapshot, seules les modifications apportées aux données d'origine (en constante évolution) par rapport à un état donné sont mises en cache ; c'est la raison pour laquelle les snapshots de type copie par écriture (copy-on-write) sans préallocation d'espace disque sont tributaires de leurs volumes source: si les données des volumes source sont perdues, les snapshots associés sont inutilisables.

Snapclones

La création des snapclones commence par une procédure semblable à celle utilisée pour créer des snapshots de type copie par écriture (copy-on-write) sans préallocation d'espace disque. Elle est suivie du processus de clonage. Pendant ce processus, toutes les données du volume source sont copiées dans le volume cible. Un snapclone permet d'accéder immédiatement aux données répliquées pendant que le processus de clonage s'exécute en tâche de fond en exploitant les périodes d'inactivité de la baie de disques. Une fois le processus de clonage achevé, le snapclone est une copie de données complète reproduisant le volume source à un état donné; si les données stockées sur le volume source sont perdues, vous pouvez toujours rétablir le snapclone.

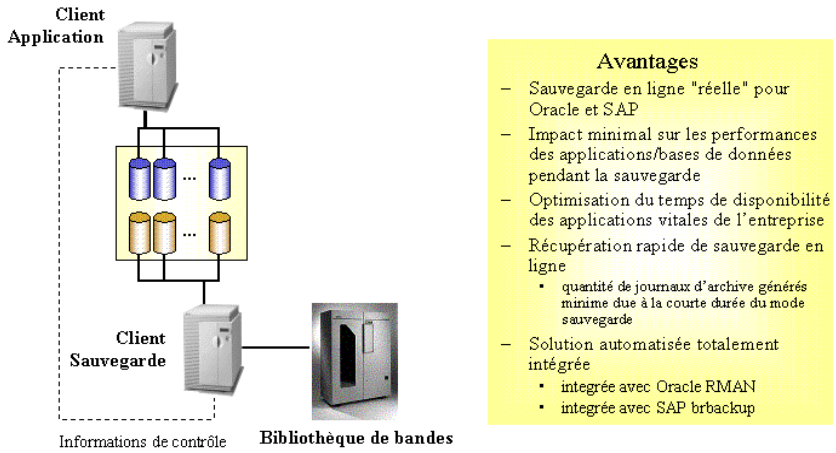
Configurations prises en charge

Configuration de base : baie de disques simple - hôte double

Les deux hôtes sont connectés à la même baie de disques, de sorte que l'infrastructure d'E/S du système RAID est partagée entre le client d'application et le client de sauvegarde.

Le client d'application et le client de sauvegarde étant deux systèmes physiquement différents, ils peuvent utiliser leurs propres ressources (canaux d'E/S, unités centrales, mémoire, etc.) pour réaliser leurs activités spécifiques, par exemple effectuer une sauvegarde, sans incidence sur le fonctionnement de l'autre. Ainsi, l'impact de la sauvegarde sur les performances de la base de données est minime.

Figure 12-2 **Baie de disques simple - hôte double (sauvegarde avec performance optimale et temps d'indisponibilité nul)**



Les fonctions de snapshot Data Protector intégrées permettent le traitement automatique de l'état des baies de disques ainsi qu'une intégration parfaite aux applications telles que SAP R/3, Oracle, Microsoft SQL ou Exchange Server (afin d'assurer la cohérence des données et la prise en compte des sauvegardes par les bases de

données/applications). Pour assurer une opération sécurisée et utiliser les outils d'application natifs pour la restauration (`sapdba`, par exemple), il faut que la sauvegarde soit prise en compte au préalable par l'application / la base de données. En cas de sauvegarde, le fonctionnement de l'application n'est affecté que le temps nécessaire pour effectuer les opérations suivantes :

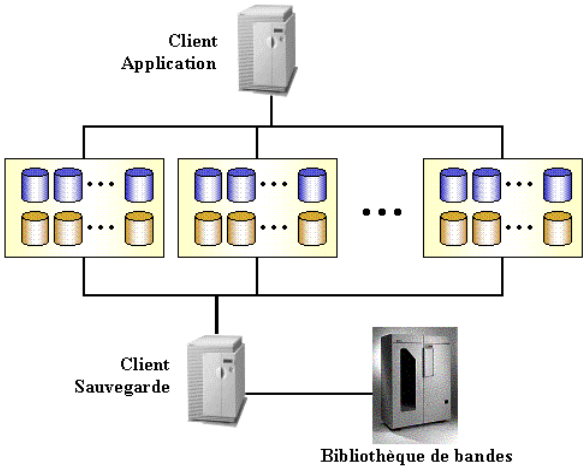
1. Réorganisation de la base de données afin d'en assurer la cohérence en vue de la génération d'un snapshot.
2. Réalisation d'un snapshot des données d'application.
3. Rétablissement du mode de fonctionnement normal de la base de données.

Cette configuration permet de réaliser en peu de temps une sauvegarde hors ligne à partir d'une base de données très volumineuse, ainsi qu'une sauvegarde en ligne générant très peu de journaux d'archive, la durée pendant laquelle la base de données reste en mode sauvegarde étant réduite au minimum.

Le fait de générer peu de journaux d'archive réduit l'espace nécessaire pour ce type de fichiers et accélère la procédure de récupération de la base de données. Après la restauration d'une base de données en ligne, il est nécessaire d'effectuer une récupération afin que les données de la base redeviennent cohérentes. Tous les journaux d'archive créés au cours de la sauvegarde doivent être utilisés. Au cours d'une sauvegarde de snapshot, seuls les journaux d'archive créés au cours du snapshot sont utilisés.

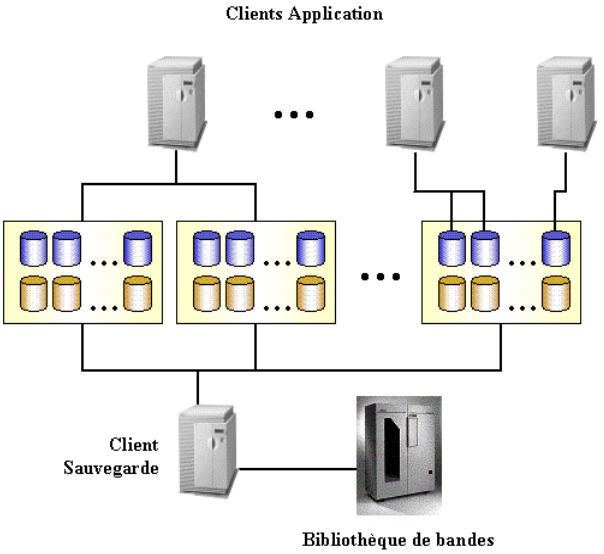
Autres configurations prises en charge

Figure 12-3 Baies de disques multiples - hôte double



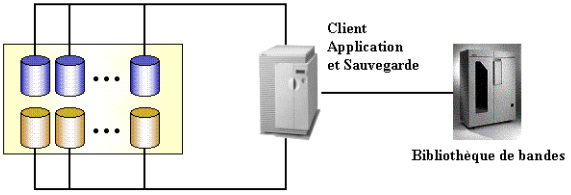
Avec cette solution, les deux hôtes sont connectés à plusieurs baies de disques. L'infrastructure d'E/S des systèmes RAID est partagée entre le client d'application et le client de sauvegarde.

Figure 12-4 Hôtes d'application multiples - hôte de sauvegarde simple



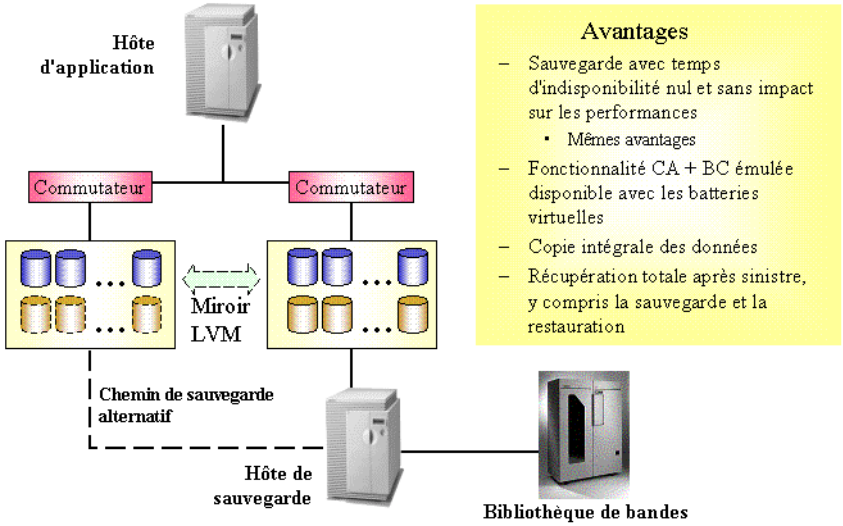
Avec cette solution, plusieurs hôtes d'application peuvent être connectés à une ou plusieurs baies de disques, elles-mêmes connectées à un hôte de sauvegarde dédié simple. L'infrastructure d'E/S des systèmes RAID est partagée entre les clients d'application et le client de sauvegarde.

Figure 12-5 Batterie(s) de disques - hôte simple



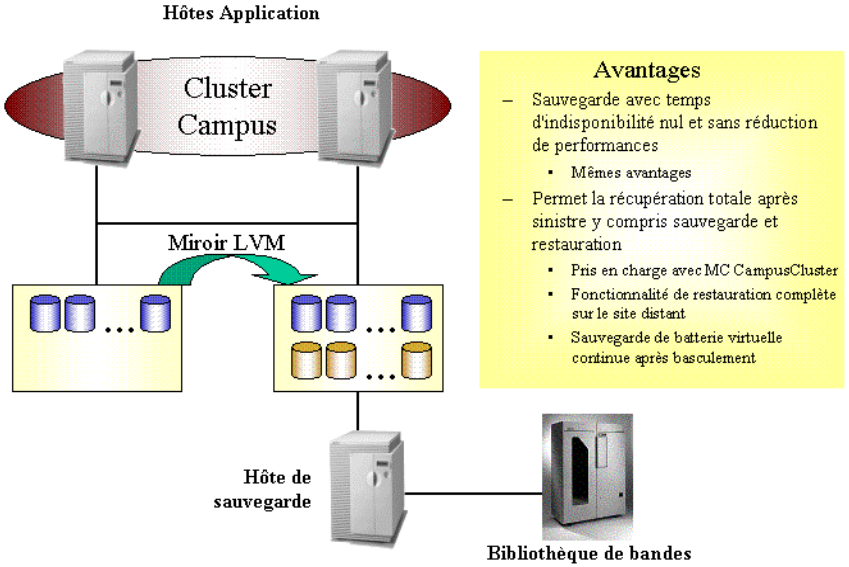
Dans les cas où aucun serveur de sauvegarde dédié n'est disponible, les deux fonctions (application et sauvegarde) peuvent être effectuées sur le même client (ou hôte). Les sauvegardes hors ligne des applications de messagerie, par exemple, peuvent réduire le temps d'indisponibilité de l'application de quelques heures à quelques minutes.

Figure 12-6 **Mise en miroir LVM - HP StorageWorks Virtual Array uniquement**



Dans le cadre des configurations prises en charge décrites précédemment, seules les fonctionnalités Business Copy peuvent être utilisées en cas d'intégration de HP StorageWorks Virtual Array. Toutefois, il est possible de recourir à la mise en miroir LVM pour créer des copies snapshots de données entre différentes baies de virtualisation, les données étant écrites sur les deux baies simultanément. Cette méthode permet l'émulation des fonctionnalités Continuous Access et Business Copy disponibles dans HP StorageWorks Disk Array XP.

Figure 12-7 **Campus Cluster et mise en miroir LVM - HP StorageWorks Virtual Array uniquement**



Cette configuration permet d'émuler les fonctionnalités Continuous Access et Business Copy, par le biais de la fonctionnalité de basculement de cluster standard. Cette fonctionnalité est souvent requise dans le cadre d'applications stratégiques.

Clients de sauvegarde et clusters

Le client de sauvegarde ne doit pas être utilisé comme serveur de basculement pour le client d'application. Il est recommandé d'installer les services d'application et de sauvegarde sur des clusters séparés.

Autres configurations

Il existe d'autres configurations de baie de disques qui fournissent des avantages spécifiques ou répondent à des besoins particuliers. Toutefois, chacune est associée à un modèle de comportement spécifique représentant des exigences particulières auxquelles les fonctions de contrôle doivent obéir afin de garantir la sauvegarde et la récupération. Il est donc important de vérifier quelles configurations sont prises en charge et de les spécifier.

Seules les configurations indiquées sont prises en charge par HP. Pour obtenir une liste récente des configurations prises en charge, consultez l'adresse suivante : http://www.openview.hp.com/products/datapro/spec_0001.html.

Si une configuration dans laquelle vous souhaitez sauvegarder des données n'est pas répertoriée dans la liste, cela ne signifie pas que l'opération ne peut pas être prise en charge. Contactez votre représentant HP local ou votre consultant HP pour connaître les autres configurations prises en charge.

13 Microsoft Volume Shadow Copy Service

Description du chapitre

Ce chapitre présente le concept de Microsoft Volume Shadow Copy service (VSS) et son rôle dans le processus de sauvegarde et de restauration. Il indique également le débit de sauvegarde et de restauration que permet cette fonction.

Le chapitre est organisé de la façon suivante :

“Présentation” à la page 333

“Intégration de Data Protector à Volume Shadow Copy” à la page 338

“Sauvegarde et restauration du système de fichiers VSS” à la page 340

Pour obtenir des informations détaillées sur l’intégration, reportez-vous au *Guide d'intégration de HP OpenView Storage Data Protector*. Pour obtenir des informations détaillées sur la sauvegarde et la restauration du système de fichiers, reportez-vous au *Guide de l’administrateur de HP OpenView Storage Data Protector*.

Présentation

Le processus de sauvegarde traditionnel est basé sur la communication directe entre l'application de sauvegarde (l'application qui lance et exécute la sauvegarde) et l'application à sauvegarder. Cette méthode de sauvegarde nécessite que l'application de sauvegarde dispose d'une interface distincte pour chaque application sauvegardée.

Le nombre d'applications présentes sur le marché ne cesse de croître. La nécessité de gérer des fonctions spécifiques à une application peut entraîner des difficultés dans les activités de sauvegarde, de restauration et de stockage. Pour résoudre ce problème, une solution efficace consiste à mettre en place un coordinateur entre les différents acteurs du processus de sauvegarde et de restauration.

VSS

Volume Shadow Copy Service (VSS) est un logiciel créé par Microsoft pour les systèmes d'exploitation Windows. Ce service collabore avec l'application de sauvegarde, les applications à sauvegarder, les fournisseurs de copies miroir et le noyau du système d'exploitation pour mettre en œuvre la gestion des copies miroir des volumes et des jeux de copies miroir.

Le logiciel Volume Shadow Copy Service vise à fournir une interface de communication unifiée, capable de coordonner la sauvegarde et la restauration de toute application, quelles que soient ses fonctionnalités spécifiques. Ainsi, l'application de sauvegarde n'a plus à gérer individuellement chaque application à sauvegarder. Toutefois, cette procédure n'est applicable à une application de sauvegarde que si celle-ci est conforme à la spécification VSS.

Qu'est-ce qu'une copie miroir ?

Le terme **copie miroir** désigne un volume représentant une copie du volume d'origine à un moment donné. La technologie de copie miroir du volume fournit une copie du volume d'origine à un moment donné. La sauvegarde de données s'effectue alors depuis la copie miroir, et non depuis le volume d'origine. Le volume d'origine change à mesure que le processus de sauvegarde se poursuit ; la copie miroir, en revanche, demeure identique.

La copie miroir n'est rien d'autre que la sauvegarde d'un snapshot, laquelle permet aux applications et aux utilisateurs de continuer à copier des données vers des volumes, même pendant un processus de sauvegarde, tandis que la sauvegarde récupère les données à partir d'une copie miroir du volume d'origine.

Un jeu de copies miroir est un ensemble de copies miroir créé au même instant.

Qu'est-ce qu'un module d'écriture ?

Le **module d'écriture** désigne tout processus apportant une modification aux données du volume d'origine. Les modules d'écriture sont habituellement des applications (telles que MSDE Writer pour MS SQL Server) ou des services système (par exemple, System Writer et Registry Writer) qui copient des informations permanentes sur un volume. Ils participent au processus de synchronisation des copies miroir en assurant la cohérence des données.

Qu'est-ce qu'un fournisseur de copie miroir ?

Le terme **fournisseur de copie miroir** désigne une entité qui exécute le travail nécessaire à la création et à la représentation des copies miroir des volumes. Les fournisseurs de copies miroir possèdent les données des copies miroir et exposent les copies miroir. Le fournisseur de copies miroir peut être de type logiciel (notamment un fournisseur de systèmes, MS Software Shadow Copy Provider) ou matériel (disques locaux, baies de disques).

La baie de disques est un exemple type de fournisseur matériel : elle possède son propre mécanisme matériel qui indique l'état d'un disque à un moment donné. Un fournisseur logiciel fonctionne sur des disques physiques et utilise un mécanisme logiciel pour fournir des indications sur l'état d'un disque à un moment donné. Le fournisseur système, MS Software Shadow Copy Provider, est un mécanisme logiciel intégré au système d'exploitation Windows Server 2003.

Le mécanisme VSS garantit que tous les fournisseurs matériels seront proposés pour la création d'une copie miroir avant tous les fournisseurs logiciels. Si aucun d'eux n'est en mesure de créer une copie miroir, VSS fait appel pour cela à MS Software Shadow Copy Provider, lequel est toujours disponible.

Data Protector et VSS

Le logiciel Volume Shadow Copy Service permet de coordonner l'application de sauvegarde, les modules d'écriture et les fournisseurs de copies miroir pendant le processus de sauvegarde et de restauration.

La figure 13-1 et la figure 13-2 présentent les différences qui existent entre le modèle de sauvegarde traditionnel et le modèle doté du coordinateur VSS.

Figure 13-1 Acteurs du modèle de sauvegarde traditionnel

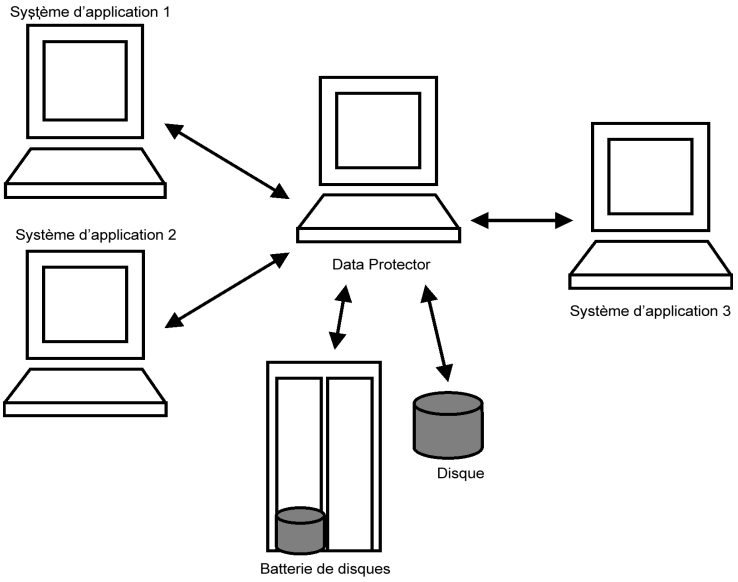
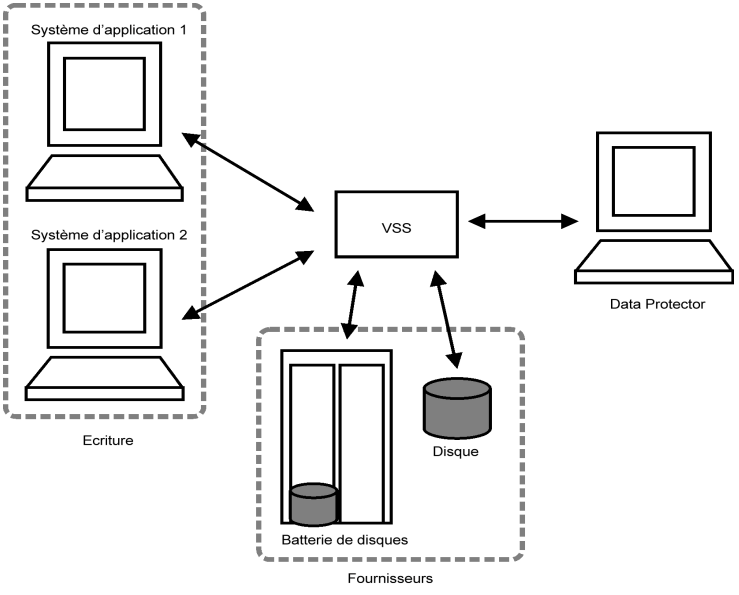


Figure 13-2 Acteurs du modèle de sauvegarde VSS



Dans le modèle traditionnel, l'application de sauvegarde devait communiquer individuellement avec chaque application qu'elle sauvegardait. Dans le modèle VSS, l'application de sauvegarde communique uniquement avec le VSS, lequel coordonne l'ensemble du processus de sauvegarde.

Avantages du VSS

Le logiciel Volume Shadow Copy service présente les avantages suivants :

- Une interface de sauvegarde unifiée est fournie à tous les modules d'écriture.
- Une interface de sauvegarde unifiée est proposée à tous les fournisseurs de copies miroir.
- L'intégrité des données est assurée au niveau de l'application par les modules d'écriture. Aucune intervention de l'application de sauvegarde n'est nécessaire.

Data Protector prend en charge le logiciel Microsoft Volume Shadow Copy service à deux niveaux :

- Au sein de l'intégration à Microsoft Volume Shadow Copy service, Data Protector fournit une sauvegarde et une restauration par copie miroir des modules d'écriture VSS.
- Au sein de la fonctionnalité Disk Agent, Data Protector fournit une sauvegarde du système de fichiers VSS.

L'intégration Data Protector VSS prend en charge une sauvegarde en copie miroir cohérente uniquement pour les modules d'écriture VSS. Dans ce cas, la cohérence est fournie du côté du module d'écriture. Lorsque les applications ne sont pas de type VSS, la copie miroir est créée, mais la cohérence des données de la copie miroir n'est pas garantie au niveau de l'application. Toutefois, la cohérence est supérieure à celle que fournirait une sauvegarde du système de fichiers de type non-VSS.

Le tableau ci-dessous met en évidence les différences entre la sauvegarde d'intégration Data Protector VSS, la sauvegarde du système de fichiers VSS et la sauvegarde du système de fichiers non-VSS :

Tableau 13-1 Avantages de l'utilisation de VSS

	Sauvegarde d'intégration Data Protector VSS	**Sauvegarde de système de fichiers VSS**	**Sauvegarde de système de fichiers non-VSS**
Fichiers ouverts	Fichiers non ouverts	Fichiers non ouverts	Si les fichiers sont ouverts, la sauvegarde risque d'échouer.
Fichiers verrouillés	Fichiers non verrouillés	Fichiers non verrouillés	Si les fichiers sont verrouillés, la sauvegarde les ignore.
Intégrité des données	Fournie par le module d'écriture.	Cohérence des données en cas de panne (par exemple, en cas de panne d'alimentation).	Aucune (inhérent)

Intégration de Data Protector à Volume Shadow Copy

L'intégration de Data Protector au logiciel Microsoft Volume Shadow Copy service offre une prise en charge complète des modules d'écriture VSS. Cela comprend la détection automatique des modules d'écriture VSS, ainsi que les fonctionnalités de sauvegarde et de restauration. Pour obtenir des informations détaillées sur l'intégration, reportez-vous au *Guide d'intégration de HP OpenView Storage Data Protector*.

Sauvegarde VSS

En cas de sauvegarde de modules d'écriture VSS, la cohérence des données est assurée au niveau du module et ne dépend pas de l'application de sauvegarde. Data Protector respecte les critères fournis par les modules d'écriture lors de la sélection des données à sauvegarder.

Au cours de la sauvegarde de modules d'écriture VSS, Data Protector ne communique pas avec chaque module d'écriture individuellement, mais via l'interface VSS. Il utilise l'agent d'intégration VSS pour connecter le service Volume Shadow Copy, lequel coordonne le processus de sauvegarde. VSS fournit à Data Protector les métadonnées liées aux modules d'écriture qui sont nécessaires à la cohérence de la sauvegarde et de la restauration. Data Protector examine ces données et identifie les volumes à sauvegarder. Ensuite, Data Protector invite VSS à créer une copie miroir des volumes spécifiés.

REMARQUE

Un **document de métadonnées de modules d'écriture** (WMD) regroupe les métadonnées fournies par chaque module d'écriture. Les modules d'écriture s'identifient par les métadonnées et indiquent à l'application de sauvegarde les données à sauvegarder et la procédure à suivre pour les restaurer. Ainsi, Data Protector se conforme aux indications fournies par le module d'écriture pour sélectionner les volumes à sauvegarder et la méthode de restauration.

Le service Volume Shadow Copy synchronise les modules d'écriture et les fournisseurs. Après la création d'une copie miroir de sauvegarde, VSS communique cette copie à Data Protector. Data Protector effectue une sauvegarde à partir du volume de copie miroir vers le support, puis informe VSS que la copie miroir peut être extraite.

Restauration VSS

La restauration d'intégration VSS fait référence à la restauration des données qui ont été sauvegardées grâce à la coordination du service Volume Shadow Copy et avec la coopération d'un module d'écriture. Pendant la procédure de restauration, le service Volume Shadow Copy coordonne les communications entre Data Protector et les modules d'écriture.

Lors de la restauration de modules d'écriture VSS, Data Protector restaure d'abord toutes les métadonnées pertinentes afin d'identifier les composants de sauvegarde et de déterminer la méthode de restauration. Il se connecte ensuite au service Volume Shadow Copy et indique que la restauration est sur le point de commencer. VSS coordonne les activités des modules d'écriture pendant la durée de la restauration. Une fois que Data Protector a correctement restauré les données, VSS informe les modules d'écriture que la restauration est terminée ; les modules d'écriture peuvent alors accéder aux données restaurées et lancer leur traitement interne.

Sauvegarde et restauration du système de fichiers VSS

Certaines applications ne détectent pas la présence du logiciel Volume Shadow Copy. Ces applications ne peuvent pas garantir la cohérence des données lors de la création des copies miroir. Le mécanisme VSS n'est pas en mesure de coordonner les activités de ces applications afin d'effectuer une sauvegarde cohérente.

Vous pouvez malgré tout bénéficier de la fonctionnalité VSS. La coopération entre l'application de sauvegarde et un fournisseur de copies miroir peut être utilisée pour garantir la plus grande cohérence possible des données. Microsoft utilise le terme "données cohérentes en cas de panne" pour qualifier cet état des données. Cela signifie que le mécanisme VSS engage toutes les opérations d'E/S en attente et interrompt les demandes d'écriture entrantes pendant la préparation d'un volume de copie miroir. Ainsi, tous les fichiers du système de fichiers sont fermés et déverrouillés pendant la création de la copie miroir.

La fonctionnalité Microsoft Volume Shadow Copy permet la création de copies miroir des volumes sans l'intervention des applications en cours de sauvegarde. Dans ce cas, le volume de copie miroir est créé, puis sauvegardé par Data Protector. Cette démarche peut être utilisée pour les applications qui ne détectent pas le mécanisme VSS.

IMPORTANT

En cas de sauvegarde d'applications qui ne détectent pas le mécanisme VSS, la cohérence des données du point de vue des applications ne peut être garantie. Les données sont aussi cohérentes qu'en cas de panne d'alimentation. Data Protector ne peut garantir la cohérence des données lorsque les applications ne participent pas activement à la création des copies miroir.

Pendant la sauvegarde du système de fichiers VSS, la cohérence des données est supérieure à celle que l'on obtient en cas de sauvegarde d'un système de fichiers non-VSS. VSS vous permet de créer des sauvegardes par copie miroir des volumes qui sont des copies exactes des fichiers à un moment donné, y compris tous les fichiers ouverts. Par exemple, les bases de données qui restent ouvertes exclusivement et les fichiers ouverts en raison de l'activité de l'opérateur ou du système sont

sauvegardés en cas de sauvegarde du système de fichiers VSS. Ainsi, les fichiers qui ont été modifiés pendant la procédure de sauvegarde sont correctement copiés.

La sauvegarde du système de fichiers VSS présente les avantages suivants :

- Il est possible de sauvegarder un ordinateur pendant que des applications et des services sont en cours d'exécution. Par conséquent, les applications peuvent continuer à écrire des données sur le volume pendant une sauvegarde.
- Les fichiers ouverts ne sont plus ignorés pendant la procédure de sauvegarde, car ils apparaissent fermés sur le volume de copie miroir au moment de la création de la copie miroir.
- Les sauvegardes peuvent être effectuées à tout moment sans obliger les utilisateurs à arrêter leur système.

Sauvegarde et restauration

La sauvegarde VSS est mise en œuvre comme une sauvegarde supplémentaire d'un système de fichiers Windows sous Windows Server 2003. Le niveau d'intégrité des données est légèrement supérieur à celui obtenu lors d'une sauvegarde traditionnelle d'un volume actif. Pour obtenir des informations détaillées sur la sauvegarde et la restauration du système de fichiers Windows, reportez-vous au *Guide de l'administrateur de HP OpenView Storage Data Protector*.

Au cours de la sauvegarde du système de fichiers VSS, les applications ne peuvent contribuer à la cohérence des données, dans la mesure où elles ne détectent pas le mécanisme VSS. Toutefois, Data Protector et un fournisseur peuvent toujours coopérer pour créer des copies miroir des volumes. La sauvegarde du système de fichiers VSS permet de sauvegarder les données telles qu'elles apparaissent à un instant T, quelle que soit l'activité d'E/S du système pendant la sauvegarde.

Lorsque Data Protector demande la sauvegarde des volumes spécifiés dans la spécification de sauvegarde, le mécanisme VSS engage toutes les opérations d'E/S en attente, interrompt les demandes d'écriture entrantes et prépare un volume de copie miroir.

Lorsque la copie miroir est créée, Data Protector lance sa procédure de sauvegarde normale, si ce n'est que le volume source est remplacé par la copie miroir qui vient d'être créée. En cas d'échec de la création de la copie miroir, Data Protector peut poursuivre la sauvegarde normale du système de fichiers, si ce comportement a été spécifié dans la spécification de sauvegarde.

Il est ainsi possible de sauvegarder un ordinateur pendant que des fichiers sont ouverts et des services en cours d'exécution. Les fichiers ne sont pas ignorés pendant une telle sauvegarde. VSS permet aux services et aux applications de continuer à fonctionner sans interruption sur les volumes réels pendant la création d'une copie miroir. Une fois la sauvegarde terminée, la copie miroir est supprimée.

La restauration de données sauvegardées à l'aide de la sauvegarde du système de fichiers VSS est similaire à la procédure de restauration standard.

A Scénarios de sauvegarde

Dans cette annexe

Vous trouverez dans cette annexe deux scénarios : l'un pour l'entreprise XYZ, l'autre pour l'entreprise ABC. Ces deux entreprises souhaitent améliorer leurs systèmes de stockage de données. Leurs solutions de sauvegarde actuelles sont décrites ainsi que les problèmes qu'elles présentent. Des solutions sont ensuite proposées pour remédier à ces problèmes et répondre aux besoins futurs de ces entreprises en matière de stockage de données.

Points à prendre en considération

Dans les deux cas, les éléments suivants sont à prendre en compte pour formuler la stratégie de sauvegarde de l'entreprise :

- Importance de la disponibilité des données du système (et de la sauvegarde) pour l'entreprise :
  - — Nécessité de conserver les données sauvegardées à un emplacement distant en cas de sinistre.
  - — Niveau de continuité des opérations, comprenant notamment un plan de récupération et de restauration pour l'ensemble des systèmes stratégiques.
  - — Sécurité des données sauvegardées

    Nécessité de contrôler l'accès aux locaux, afin d'en interdire l'entrée à toute personne non autorisée. Cela comprend également la protection des données pertinentes contre tout accès non autorisé, à l'aide de dispositifs physiques empêchant d'y accéder et d'une protection électronique par mot de passe.
- Types de données à sauvegarder :

  Vous pouvez regrouper les données en catégories, telles que Données commerciales, Données de ressources de l'entreprise, Données de projet et Données personnelles, chacune de ces catégories ayant des besoins spécifiques.
- Facteurs de performance pour la sauvegarde et la restauration :
  - — Topologie réseau et système

Déterminez quels systèmes peuvent utiliser quels liens réseau, et quels taux de transfert sont possibles.

— La fenêtre temporelle

Définissez les périodes au cours desquelles les sauvegardes de systèmes spécifiques peuvent être effectuées.

— Sauvegardes locales ou réseau

Parmi les systèmes auxquels sont connectés des périphériques de sauvegarde, déterminez lesquels seront sauvegardés en local et lesquels seront sauvegardés sur le réseau.

- Mise en œuvre de la stratégie de sauvegarde :

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

  Ces critères permettent de définir la fréquence des sauvegardes complètes et incrémentales, les options de sauvegarde à utiliser, et si les données sauvegardées doivent ou non être protégées définitivement à l'aide de supports stockés sur un site distant.

  — Comment regrouper les systèmes dans des spécifications de sauvegarde ?

  Etudiez la meilleure manière de regrouper les spécifications de sauvegarde (par service, par type de données ou par fréquence de sauvegarde).

  — Comment planifier les sauvegardes ?

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

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

  Pensez à protéger les données pendant une période spécifique contre tout risque d'écrasement lors de nouvelles sauvegardes.

  Définissez la période à laquelle la base de données catalogue Data Protector doit stocker les informations sur les sauvegardes.

- Configuration des périphériques

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

  Si vous devez sauvegarder de grandes quantités de données, pensez à utiliser un périphérique de bibliothèque.

- Gestion des supports

  Déterminez le type de support à utiliser, ainsi que la manière de regrouper les supports en pools et de placer les objets sur ces supports.

- Mise au coffre

  Décidez si les supports doivent être stockés en lieu sûr, où ils seront conservés durant une période déterminée.

- Administrateurs et opérateurs de sauvegarde

  Définissez les droits d'administration et d'accès pour les utilisateurs des systèmes de sauvegarde.

Entreprise XYZ

XYZ est une agence de traduction proposant les services suivants :

- Traduction, localisation, adaptation linguistique et relecture.
- Certification de documents traduits.
- Interprétation consécutive et simultanée.
- Publication et graphisme assistés par ordinateur.
- Location de matériel pour l'interprétation de conférence.

La croissance annuelle de XYZ se situe actuellement entre 20 et 25 %, mais sa solution de sauvegarde n'est pas adaptée au rythme de cette croissance. Le processus de sauvegarde requiert l'intervention d'un personnel nombreux, car les bandes de sauvegarde doivent être gérées manuellement.

Environnement

Cette section décrit l'environnement matériel et logiciel actuel de XYZ, et la manière dont est mise en œuvre la stratégie de stockage des données.

XYZ est divisée en trois services connectés à un réseau d'entreprise principal :

- Le service Anglais.
- Le service Autres langues.
- Le service Administration.

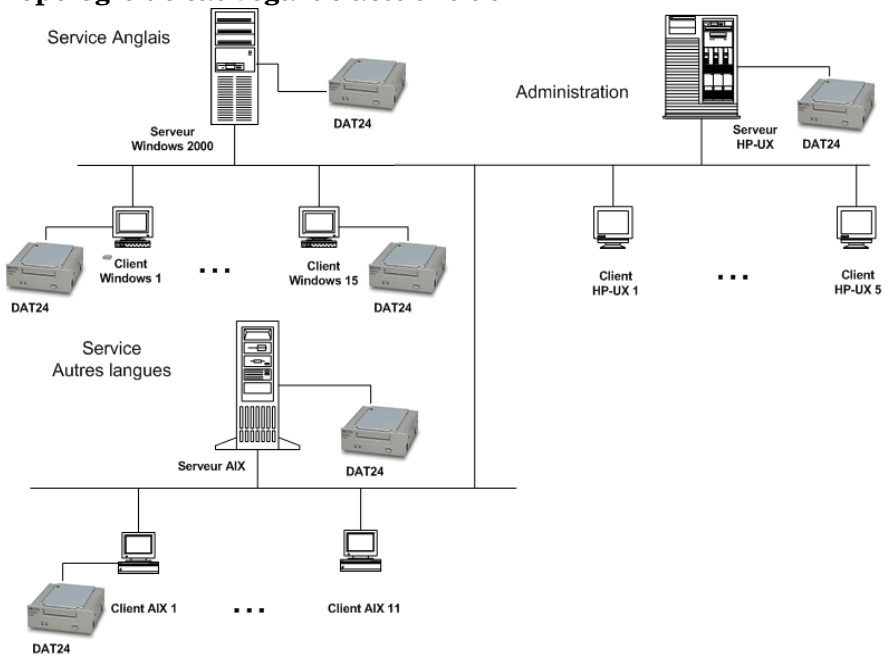
Vous trouverez la description de l'environnement matériel et logiciel d'XYZ dans le tableau A-1 à la page A-6, et celle de sa topologie de sauvegarde actuelle à la figure A-1 à la page A-7.

Tableau A-1 Environnement matériel et logiciel de XYZ

Service	Nb de serveurs	Nb de clients	Qté de données actuelle	Qté de données prévue (dans 5 ans)	Périphériques actuels
Anglais	1 Windows 2000	15 Windows	35 Go	107 Go	3 chargeurs automatiques HP StorageWorks DAT24
Autres langues	1 AIX	11 UX	22 Go	67 Go	2 chargeurs automatiques HP StorageWorks DAT24
Administration	1 HP-UX	5 UX	10 Go	31 Go	1 chargeur automatique HP StorageWorks DAT24

La figure A-1 à la page A-7 présente l'organisation de l'environnement de sauvegarde de XYZ.

Figure A-1 **Topologie de sauvegarde actuelle de XYZ**



XYZ dispose actuellement de trois serveurs pour un volume de données total estimé à 67 Go. Dans le service Anglais, chaque employé copie manuellement les données tous les soirs sur son serveur respectif. L'un des clients Windows 2000 de ce service assure le stockage d'environ un tiers des données (12 Go).

La sauvegarde des systèmes clients du service Autres langues s'effectue via un NFS (Network File System), tandis que celle des systèmes client du service Administration s'effectue par le biais de partages réseau. Les employés du service Autres langues travaillent également le samedi.

Problèmes rencontrés avec la solution actuelle

La solution de sauvegarde actuelle n'est pas adaptée au rythme de la croissance de XYZ. Le processus de sauvegarde actuel nécessite beaucoup de travail manuel. Il ne permet pas d'améliorer la gestion de la sauvegarde ni d'installer une architecture de sauvegarde unique pour l'ensemble de l'entreprise. Chacun des serveurs de sauvegarde est géré séparément. Il est impossible de centraliser la gestion de sauvegarde.

Voici quelques-uns des problèmes liés à la solution actuelle :

- La solution de sauvegarde n'est pas automatisée.
  - — Les employés doivent copier leur travail régulièrement, ce qui augmente les risques d'erreur.
  - — Les utilitaires de sauvegarde ne sont pas les mêmes, ce qui entraîne un accroissement des coûts de formation.
- Les solutions utilisées dans le service Autres langues et le service Administration sont plus élaborées mais présentent également des problèmes spécifiques. L'utilisation du réseau influe considérablement sur les performances de sauvegarde. De plus, toutes les données ne sont pas sauvegardées. Seuls les fichiers partagés via le Network File System sont sauvegardés dans le service Autres langues, et seuls les fichiers partagés sur réseau sont sauvegardés dans le service Administration.
- Les trois services utilisant chacun un serveur de sauvegarde indépendant, il n'y a pas de centralisation du contrôle ni de la gestion des opérations clés suivantes :
  - — Configuration des périphériques.
  - — Gestion des supports.
  - — Configuration de sauvegarde.
  - — Planification.
  - — Surveillance.
  - — Opérations de restauration.
- Chaque serveur de sauvegarde étant géré individuellement, la génération des rapports n'est pas centralisée.
- La solution actuelle n'offre aucune fonction de récupération après sinistre, ce qui constitue un inconvénient de plus en plus important. En effet, un sinistre peut entraîner la perte d'une partie essentielle du travail de l'entreprise.

Besoins relatifs à une stratégie de sauvegarde

Besoins

Après avoir pris en compte les éléments énumérés à la section "Points à prendre en considération" à la page A-2, nous avons identifié les besoins suivants pour la solution de sauvegarde de l'entreprise XYZ :

- Stratégie de sauvegarde :
  - — Des sauvegardes hebdomadaires complètes seront réalisées en l'espace de 12 heures.
  - — Des sauvegardes incrémentales quotidiennes seront réalisées en l'espace de 8 heures à la fin de chaque journée de travail.
  - — Une période fixe pour la protection des données sera mise en place.
  - — Les supports de sauvegarde seront stockés sur un site distant.
- Sauvegarde :

  Toutes les opérations de sauvegarde doivent nécessiter moins d'intervention manuelle qu'actuellement.
- Restauration
  - — Une restauration pratique et rapide doit être proposée. Les données à restaurer doivent pouvoir être explorées pendant les trois semaines suivant la sauvegarde.
  - — La restauration des sauvegardes de données placées dans le coffre doit être possible en deux jours.
- Connexion réseau :

  Les agents de support et les services seront connectés à un réseau local Ethernet 100TX.
- Croissance prévue :

  On prévoit 20 à 25 % d'augmentation annuelle des capacités de données pour les cinq années à venir.
- Logiciels :

  Les serveurs de sauvegarde doivent s'exécuter sur l'un des systèmes d'exploitation pris en charge. Pour obtenir des informations sur les systèmes d'exploitation pris en charge pour le Gestionnaire de cellule, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector*.
- Protection contre un sinistre :

  Une fois les sauvegardes terminées, les supports seront stockés sur site où ils pourront être récupérés à la demande pour la restauration de fichiers. Au bout de 20 jours, ils seront déplacés vers un lieu de

stockage hors site afin d'être protégés en cas de sinistre dans l'entreprise, et afin de libérer de la place pour de nouveaux supports de sauvegarde.

Solution proposée

Etant donné les performances limitées de la solution actuelle et l'impossibilité d'une gestion centralisée, XYZ doit revoir la conception de son architecture et de sa stratégie de sauvegarde afin de pouvoir atteindre ses objectifs commerciaux. La solution proposée est d'abord présentée dans son ensemble, puis en détails. Notez qu'il s'agit d'une proposition et non de la seule solution possible aux problèmes de gestion de stockage de XYZ.

Présentation générale de la solution

Tous les clients et serveurs doivent être configurés dans une seule cellule Data Protector avec le serveur Windows 2000 du service Anglais, utilisé à la fois comme Gestionnaire de cellule et comme Serveur d'installation pour les systèmes Windows. Utilisez le serveur de sauvegarde HP-UX du service Administration comme Serveur d'installation pour les systèmes UNIX. Les périphériques de sauvegarde sont les suivants : une bibliothèque HP StorageWorks DLT 4115w et deux des chargeurs automatiques HP StorageWorks DAT24 utilisés jusqu'à présent.

Ce matériel est suffisant pour les cinq années à venir au taux de croissance actuel de 20 à 25 % par an. L'utilisation de périphériques existants constitue un avantage supplémentaire dans le cas d'une récupération après sinistre. Le client Windows 2000, qui comporte environ un tiers des données du service Anglais (12 Go), doit être sauvegardé en local sur un chargeur automatique HP StorageWorks DAT24. La solution de sauvegarde proposée offre les avantages suivants :

- Sauvegardes très performantes ;
- Gestion des supports avec intervention minimale du personnel ;
- Récupération après sinistre simple et efficace ;
- Génération centralisée de rapports sur les sauvegardes ;
- Automatisation de la plupart des opérations de sauvegarde.

Toutes ces opérations sont réalisées avec une seule solution, en association avec le matériel proposé :

Tableau A-2 Environnement proposé

Service	Qté de données actuelle	Qté de données prévue (dans 5 ans)	Périphériques	
Anglais*	35 Go	107 Go	Bibliothèque HP DLT 4115	2 chargeurs automatiques HP StorageWorks DAT24
Autres langues	22 Go	67 Go		
Administration	10 Go	31 Go		
* Un chargeur automatique HP StorageWorks DAT24 est actuellement utilisé pour sauvegarder en local les 12 Go de données. L'autre chargeur automatique HP StorageWorks DAT24 est utilisé pour sauvegarder les fichiers de configuration et la base de données IDB. Les autres données du service sont sauvegardées à distance vers la bibliothèque HP StorageWorks DLT 4115.				

Les quatre autres chargeurs automatiques HP StorageWorks DAT24 sont utilisés sur un système R. et D. séparé qui n'est pas intégré à la configuration proposée.

L'un des composants logiciels proposés pour la solution de sauvegarde d'entreprise est HP OpenView Storage Data Protector A.05.50.

Description détaillée de la solution proposée

La solution proposée est décrite en détail ci-dessous :

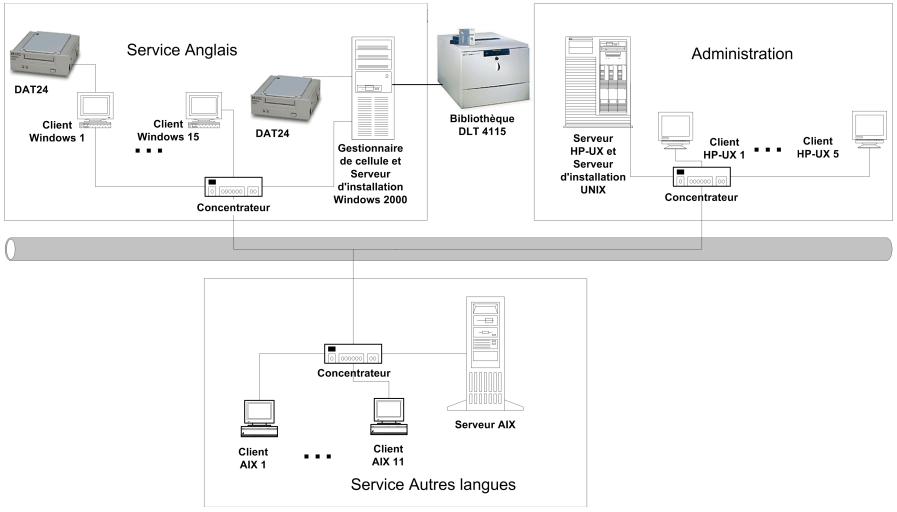
- Configuration de la cellule

  Tous les clients et serveurs doivent être configurés dans une seule cellule Data Protector. Le Gestionnaire de cellule Data Protector devrait fonctionner sur le serveur Windows 2000 du service Anglais.

Pour des performances optimales, tous les systèmes de la cellule doivent se trouver sur le même réseau local. Le Gestionnaire de cellule doit également être utilisé comme Serveur d'installation pour Windows. Utilisez le serveur de sauvegarde HP-UX du service Administration comme Serveur d'installation pour UNIX. La bibliothèque HP StorageWorks DLT 4115w doit être connectée au Gestionnaire de cellule, de même qu'un chargeur automatique HP StorageWorks DAT24 pour la sauvegarde des fichiers de configuration et de la base de données IDB. Le client Windows 2000, qui comporte environ un tiers des données du service Anglais (12 Go), doit être sauvegardé en local sur un chargeur automatique HP StorageWorks DAT24.

L'environnement de sauvegarde proposé est illustré par la figure A-2 à la page A-12 :

Figure A-2 Topologie de sauvegarde proposée pour XYZ



Le Gestionnaire de cellule gère la base de données catalogue (CDB). Cela permet de disposer pendant au moins 20 jours du détail des fichiers et des répertoires dans la base de données en cours.

Estimation de la taille de la base de données IDB

L'outil de planification de capacité de la base de données interne a été utilisé pour estimer la taille atteinte par la base de données IDB en une année. Cet outil est situé dans le même répertoire que les autres manuels Data Protector en ligne. Les paramètres d'entrée présentés à la

figure A-3 à la page A-13 comprennent le nombre de fichiers dans l'environnement (2 millions), le facteur de croissance (1,2), la protection des données (52 semaines), la protection de catalogue (3 semaines), le nombre de sauvegardes complètes hebdomadaires (1), et le nombre de sauvegardes incrémentales hebdomadaires (5).

Figure A-3 Paramètres d'entrée

Description de l'environnement			
	Fichiers :	2	**millions**
	Fichiers par répertoire :	10	
	Volume de données :	200	**Go**
	Facteur de croissance :	1,20	
	Performances du périph. :	10,00	**Mo/s**
	Capacité du support :	70,00	**Go**
	Objets :	50	
	Modif. par sauv. incrément. :	5,00%	
Paramètres de sauvegarde			
	Périphériques simult. :	2	
	Taille segment données :	2048,00	**Mo**
	Niveau de journalisation :	Tout	
	Protection des données :	52	**semaines**
	Protection du catalogue :	3	**semaines**
	Sauv. complètes/semaine :	1	
	Sauv. incrémentielles/sem. :	5	
Param. du Gestionnaire de cellule	**Vitesse d'insertion :**	12	**millions/h**

Les résultats sont présentés à la figure A-4 à la page A-14. En une année, la base de données devrait croître pour atteindre environ 419,75 Mo.

Figure A-4 **Résultats**

Résultats/calculs			
	Taille de fichier moy. :	123,36	Ko
	Fichiers/segment :	16931,38	
	Taille de catalogue :	1,03	Mo
	Périphériques K :	40	
	Performances K :	1445,647059	Go/h
	Durée K :	0,14	heure
	Supports protégés :	278,5714286	

Estimation espace			
MMDB :		30,00	Mo
CDB :	Fnames :	153,00	Mo
	Overs :	5,71	Mo
	Mpos :	1,54	Mo
DCBF :		229,50	Mo
SMBF :		2,86	Mo
Total :		419,75	Mo

- Matériel
  - — Réseau

    Pour des performances optimales, l'ensemble des systèmes doit se trouver sur le même réseau 100TX. Ce réseau présente un taux de transfert de données de 10 Mo/s ou 36 Go/h.
  - — Périphériques de sauvegarde

    Les périphériques de sauvegarde sont les suivants : une bibliothèque HP StorageWorks DLT 4115w et deux chargeurs automatiques HP StorageWorks DAT24.

Pourquoi utiliser la bibliothèque HP StorageWorks DLT 4115w ?

La bibliothèque HP StorageWorks DLT 4115w dispose d'un seul lecteur DLT4000 doté de 15 emplacements. Elle présente une capacité totale de stockage compressé de 600 Go et un taux de transfert maximum de 3 Mo/s, ou 10,5 Go/h, avec compression de données. Il s'agit du taux sur lequel nous nous baserons pour la suite de cette section. Actuellement, la quantité totale de données à sauvegarder vers la bibliothèque HP StorageWorks DLT 4115w dans le cadre d'une sauvegarde complète, qu'il s'agisse d'une seule sauvegarde ou d'une sauvegarde échelonnée, est d'environ 55 Go. En supposant que la taille d'une sauvegarde incrémentale corresponde à environ 5 % de celle d'une sauvegarde complète, une génération de sauvegarde, c'est-à-dire une sauvegarde complète plus toutes les sauvegardes incrémentales qui en découlent, nécessite un

espace de (55 + 55 x 5 % x 5) Go, soit **68,75 Go**, dans la bibliothèque. D'ici cinq ans, cet espace nécessaire devrait augmenter pour atteindre environ 210 Go. La stratégie de sauvegarde de XYZ nécessite la conservation de deux générations de sauvegardes de données. Un espace de 210 x 2 Go, soit 420 Go, est donc nécessaire dans la bibliothèque pour le stockage. La capacité de stockage (600 Go) de la bibliothèque HP StorageWorks DLT 4115w est donc suffisante.

Pourquoi utiliser le chargeur automatique HP StorageWorks DAT24 ?

Le chargeur automatique HP StorageWorks DAT24 est doté de six cartouches de données de 24 Go. Elle présente une capacité totale de stockage compressé de 144 Go et un taux de transfert maximum de 2 Mo/s, ou 7 Go/h, avec compression de données. Il s'agit du taux sur lequel nous nous baserons pour la suite de cette section. Actuellement, la quantité totale de données à sauvegarder vers le chargeur automatique HP StorageWorks DAT24 (connecté au client Windows 2000 du service Anglais mentionné plus haut) dans le cadre d'une seule sauvegarde complète est de 12 Go. En supposant que la taille d'une sauvegarde incrémentale corresponde à environ 5 % de celle d'une sauvegarde complète, une génération de sauvegarde, c'est-à-dire une sauvegarde complète plus toutes les sauvegardes incrémentales qui en découlent, nécessite un espace de (12 + 12 x 5 % x 5) Go, soit **15 Go**. D'ici cinq ans, cet espace nécessaire devrait augmenter pour atteindre environ 45 Go. La stratégie de sauvegarde de XYZ nécessite la conservation de deux générations de sauvegardes de données. Un espace de 45 x 2 Go, soit **90 Go**, est donc nécessaire dans la bibliothèque pour le stockage. La capacité de stockage (144 Go) du chargeur automatique HP StorageWorks DAT24 est donc suffisante.

Combien de temps dure une sauvegarde complète ?

Le client Windows 2000 du service Anglais, sur lequel sont stockés 12 Go de données, doit être sauvegardé en local sur un chargeur automatique HP StorageWorks DAT24. Ce périphérique présente un taux de transfert de données de 2 Mo/s ou 7 Go/h environ. Par conséquent, la sauvegarde complète de ce client Windows 2000 prend environ **2 heures**. La quantité de données augmentant de 20 à 25 % par an, il est prévu que ce client contienne environ 36 Go de données dans cinq ans. La sauvegarde de ces données prendrait alors **6 heures**.

La base de données catalogue Data Protector a une taille d'environ 0,4 Go. Elle est sauvegardée en local sur un chargeur automatique HP StorageWorks DAT24 dont le taux de transfert de données est de 2 Mo/s, ou 7 Go/h. Par défaut, Data Protector vérifie l'intégrité de la base de données avant sa sauvegarde. La vérification de l'intégrité d'une base de données de 0,4 Go prend moins d'une demi-heure, et sa sauvegarde seulement quelques minutes. Ainsi, le processus de vérification et de sauvegarde de la base de données IDB et des fichiers de configuration dure moins d'**une heure**.

Dans cinq ans, la taille de la base de données devrait atteindre 1,2 Go. La vérification de l'intégrité d'une base de données de 1,2 Go prend moins d'une heure, et sa sauvegarde moins d'une demi-heure. Ainsi, le processus de vérification et de sauvegarde de la base de données IDB et des fichiers de configuration dure moins de **2 heures**.

Toutes les autres données disponibles sur le système (représentant actuellement 55 Go environ) sont sauvegardées à distance vers la bibliothèque HP StorageWorks DLT 4115w, dont le taux de transfert est de 3 Mo/s, ou 10,5 Go/h. La plupart de ces données transitent par le réseau 100TX, dont le taux de transfert est de 10 Mo/s, ou 36 Go/h. Il n'y a pas de goulet d'étranglement. La sauvegarde de toutes ces données devrait donc prendre entre **5 et 7 heures** environ, ce qui est inférieur aux 12 heures autorisées. Un problème se pose toutefois : lorsque les données atteindront 170 Go comme prévu dans cinq ans, la sauvegarde durera entre 15 et 21 heures !

Pour remédier à ce problème, adoptez l'approche échelonnée. Planifiez la sauvegarde complète des données du service Anglais pour chaque vendredi à 20:00, celle des données du service Autres langues pour chaque samedi à 20:00 et celle des données du service Administration pour chaque dimanche à 20:00.

Tableau A-3 Approche échelonnée

	Lun	Mar	Mer	Jeu	Ven	Sam	Dim
Anglais	Incr1	Incr1	Incr1	Incr1	Complète	Incr1	
Autres langues	Incr1	Incr1	Incr1	Incr1	Incr1	Complète	
Administration	Incr1	Incr1	Incr1	Incr1	Incr1		Complète

Le tableau A-4 à la page A-17 présente les caractéristiques en matière de quantité de données et de durée pour les sauvegardes complètes effectuées aujourd'hui, ainsi que pour celles effectuées d'ici à cinq ans.

Tableau A-4 Sauvegardes complètes à distance vers la bibliothèque HP DLT 4115

Service	Qté de données actuelle/Durée de la sauvegarde	Données prévues/Durée de la sauvegarde
Anglais	23 Go / 3 h	70 Go / 7 h
Autres langues	22 Go / 3 h	67 Go / 7 h
Administration	10 Go / 1 h	31 Go / 3 h

En supposant que la taille d'une sauvegarde incrémentale corresponde à 5 % de celle d'une sauvegarde complète, la durée pour une sauvegarde complète de toutes les données sauvegardées à distance dans le service le plus important (Anglais), ainsi que des sauvegardes incrémentales des deux autres services, devrait atteindre dans cinq ans 7 + 5 % (7 + 0,35) heures, soit à moins de 8 heures, ce qui est inférieur aux 12 heures autorisées.

- Pools de supports

  Les supports sont regroupés dans des pools pour être mieux suivis et contrôlés. Regroupez les supports du même type (DLT ou DDS) dans leurs pools respectifs.

  — DDS par défaut

  Ce pool doit être utilisé pour tous les supports DDS.

  — DLT par défaut

  Ce pool doit être utilisé pour tous les supports DLT.

  — DB_Pool

  Ce pool doit être utilisé pour les fichiers de configuration et la base de données IDB. Pour des raisons de sécurité, il est recommandé de sauvegarder la base de données sur deux supports.

- Spécifications de sauvegarde

  Configurez cinq spécifications de sauvegarde, une pour chaque service, et une pour les fichiers de configuration et la base de données IDB :

  — ENG1_BS :

  Spécification de sauvegarde pour le client Windows 2000 à sauvegarder en local dans le service Anglais. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète chaque vendredi et une sauvegarde incrémentale de niveau 1 tous les jours à 20:00, sauf le vendredi et le dimanche.

Pourquoi utiliser des sauvegardes incrémentales de niveau 1 ?

Pour restaurer les données les plus récentes, seuls deux jeux de supports sont nécessaires : l'un pour la dernière sauvegarde complète et l'autre pour la dernière sauvegarde incrémentale de niveau 1 précédant la restauration. Cela permet de simplifier et d'accélerer considérablement le processus de restauration.

  — ENG2_BS :

  Spécification de sauvegarde pour les données du service Anglais devant être sauvegardées à distance vers la bibliothèque HP StorageWorks DLT 4115w. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète chaque vendredi et des sauvegardes incrémentales de niveau 1 tous les jours à 20:00, sauf le dimanche.

  — OTH_BS :

  Spécification de sauvegarde pour les données du service Autres langues devant être sauvegardées à distance vers la bibliothèque HP StorageWorks DLT 4115w. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète chaque samedi à 20:00 et des sauvegardes incrémentales de niveau 1 tous les jours à 20:00, sauf le dimanche.

  — ADM_BS :

  Spécification de sauvegarde pour les données du service Administration devant être sauvegardées à distance vers la bibliothèque HP StorageWorks DLT 4115w. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète chaque dimanche à 20:00 et des sauvegardes incrémentales de niveau 1 tous les jours à 20:00, sauf le samedi.

— DB_BS :

Spécification de sauvegarde pour les fichiers de configuration et la base de données IDB. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète tous les jours à 04:00. A cette heure, les autres sauvegardes complètes et incrémentales seront terminées et aucun problème lié au partage des ressources processeur ne se présentera entre le Gestionnaire de cellule et les autres systèmes client. Il est recommandé de faire deux copies de la base de données.

Options de sauvegarde

Utilisez les options de sauvegarde Data Protector par défaut. Définissez les options comme suit :

— Protection de catalogue

La protection de catalogue permet de définir l'intervalle de temps au cours duquel la base de données catalogue Data Protector doit conserver les informations sur les versions sauvegardées, sur le nombre de fichiers et de répertoires sauvegardés et sur les messages stockés dans la base de données. A l'expiration de la protection de catalogue, il n'est plus possible d'explorer les fichiers et répertoires à l'aide de l'interface Data Protector. Choisissez une protection de 20 jours.

— Protection de données

La protection de données détermine l'intervalle de temps au cours duquel un support ne peut pas être réutilisé. Choisissez une protection de données permanente afin de vous assurer que les données figurant sur les supports ne soient pas écrasées involontairement.

— Simultanéité :

Réglez sur 5 le nombre d'Agents de disque pouvant écrire simultanément des données dans la bibliothèque HP StorageWorks DLT 4115w. Vous améliorerez ainsi les performances de sauvegarde.

— Pool de supports :

Pour la base de données IDB, sélectionnez le pool DB_Pool contenant les supports appropriés à utiliser. Pour d'autres objets, utilisez les pools de supports par défaut.

Options de restauration

Utilisez les options de restauration Data Protector par défaut. Définissez les options comme suit :

— Lister fichiers restaurés

Activez cette option pour obtenir la liste des chemins d'accès des fichiers et répertoires restaurés. Lorsque les fichiers à restaurer sont trop nombreux, cette opération peut ralentir la procédure de restauration.

— Afficher statistiques

Activez cette option pour afficher les statistiques détaillées sur une session de restauration particulière, notamment le nombre de fichiers et de répertoires restaurés et la quantité de données restaurées.

- Génération de rapports et notification

  Des notifications envoyées par e-mail aux administrateurs de sauvegarde sont définies pour les demandes de montage, en cas d'espace insuffisant dans la base de données, en cas d'erreurs de périphériques et à la fin des sessions pour toutes les spécifications de sauvegarde. Eventuellement, des notifications par e-mail ou message de diffusion sont définies pour les utilisateurs finaux souhaitant être informés de la réussite des sauvegardes de leurs systèmes.

  Pour permettre à tous les utilisateurs de connaître facilement l'état de leurs sauvegardes, définissez les informations de sauvegarde client sur l'Intranet de l'entreprise comme suit :

  1. Configurez un groupe de rapports avec un rapport sur la sauvegarde client pour chaque client. Le rapport doit être enregistré dans le fichier au format HTML.
  2. Planifiez le groupe de rapports.
  3. Reliez les fichiers contenant les rapports à la page Intranet de l'entreprise.

- Mise au coffre

  La mise au coffre consiste à stocker des supports en lieu sûr pendant une période déterminée.

  Des supports seront déplacés vers le coffre une fois par semaine, et remplacés par de nouveaux supports dans la bibliothèque HP StorageWorks DLT 4115w et les chargeurs automatiques

HP StorageWorks DAT24. Toutes les actions, hormis le déplacement de supports vers le coffre, sont exécutées par la solution logicielle, y compris les requêtes effectuées en interne dans la base de données pour éviter à l'administrateur d'avoir à rechercher les supports devant être éjectés.

Le second déplacement des supports s'effectue du coffre vers une entreprise de sécurité. Celui-ci a lieu une fois par mois. Data Protector publie un rapport sur les supports devant être déplacés vers l'entreprise de sécurité.

Effectuez le suivi des supports déplacés vers un coffre. Cette opération est utile lorsque vous souhaitez restaurer des données à partir de sauvegardes réalisées sur un support déplacé vers une entreprise de sécurité. Data Protector vous permet d'effectuer les tâches de mise au coffre suivantes :

— Génération de rapports sur les supports stockés à un endroit spécifique et dont la protection de données expire à une date déterminée.

— Génération de rapports sur les supports utilisés pour une sauvegarde au cours d'une période donnée.

— Affichage d'une liste de spécifications de sauvegarde ayant utilisé des supports spécifiques lors de la sauvegarde.

— Affichage d'une liste de supports nécessaires pour les opérations de restauration et des emplacements physiques où sont stockés ces supports.

— Filtrage des supports à partir de l'affichage des supports selon des critères spécifiques (affichage des supports dont la protection a expiré, par exemple).

- Restauration

  — Restaurer par requête :

  Les demandes de restauration par requête sont envoyées à l'administrateur. Si la dernière sauvegarde des fichiers date de moins de 20 jours avant l'émission de la requête, l'administrateur peut utiliser l'option Restaurer par requête pour sélectionner les fichiers et répertoires à restaurer selon des critères particuliers. Il choisit ensuite l'option Ecraser pour remplacer les fichiers et répertoires du disque par les versions figurant sur le support.

— Restauration complète de système de fichiers :

Les demandes de restauration de systèmes de fichiers entiers sont envoyées à l'administrateur. Si la dernière sauvegarde des fichiers date de moins de 20 jours avant l'émission de la requête, l'administrateur peut sélectionner les objets à restaurer et utiliser l'option Restaurer dans.

Les objets sont alors restaurés avec la même structure de répertoires dans un répertoire sélectionné. Servez-vous d'un utilitaire Windows ou UNIX pour comparer les objets restaurés aux objets sauvegardés.

— Restauration à partir d'un coffre :

Pour restaurer des données à partir d'un coffre (sauvegardées, par exemple, 3 ans auparavant), envoyez une requête à l'administrateur. Celui-ci effectue alors les opérations suivantes :

1. Il identifie les supports nécessaires à la restauration.
2. Il déplace les supports du coffre vers la bibliothèque HP StorageWorks DLT 4115w ou vers un autre périphérique, puis les analyse.
3. Si le support ne se trouve pas dans la base de données IDB, il sélectionne l'objet spécifique à restaurer à l'aide de l'option Lister depuis supports.
4. Il effectue la restauration.

Entreprise ABC

ABC est une entreprise de génie logiciel à forte croissance dont le siège social se trouve au Cap, en Afrique du sud. En tant que prestataire (outsourcer) au service de partenaires multinationaux, ABC met en place des équipes de projets multi-sites ainsi que l'infrastructure associée pour mener à bien, en toute transparence, une vaste gamme de projets de génie logiciel. La croissance actuelle d'ABC est de 30 à 40 % par an. On pense que ce rythme va diminuer pour revenir à 15 à 20 % dans les cinq ans à venir.

Environnement

Cette section décrit l'environnement matériel et logiciel actuel d'ABC ainsi que la manière dont est mise en œuvre la stratégie de stockage des données.

ABC possède des bureaux en trois endroits. Les principales données matérielles relatives à ces trois bureaux sont affichées dans le tableau A-5 à la page A-23.

Tableau A-5 Taille de l'environnement de sauvegarde

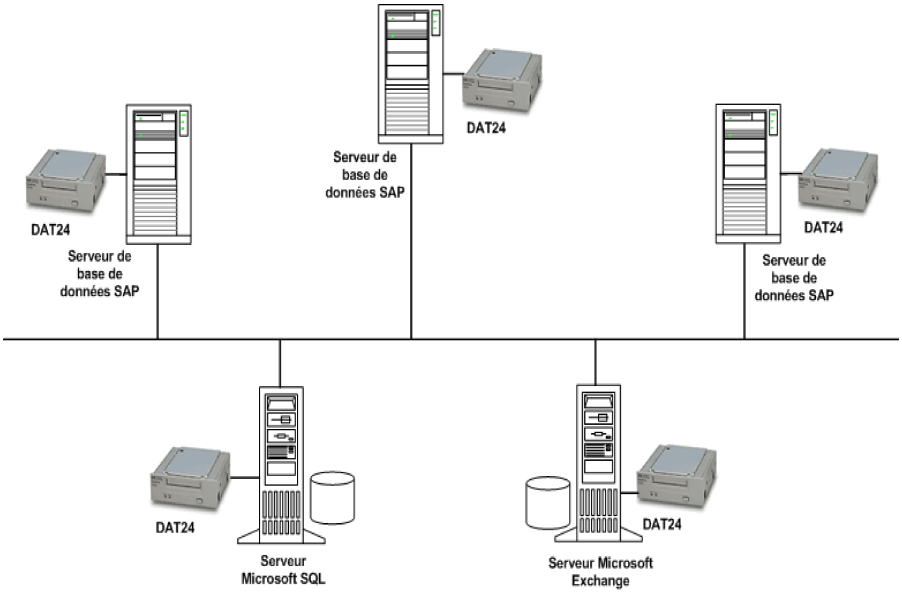
Lieu	Nb de serveurs Win	Nb de clients Win	Nb de serveurs UX	Nb de clients UX	Qté de données actuelle	Qté de données dans 5 ans	Périphériques actuels
ABC Le Cap	7	55	11	40	100	250	5 DAT24*
ABC Pretoria	5	39	5	32	22	55	1 DAT24*
ABC Durban	3	21	6	59	16	40	1 DAT24*
* Chargeur automatique HP StorageWorks DAT24							

Trois services d'ABC Le Cap utilisent la base de données Microsoft SQL pour stocker leurs données, et l'entreprise utilise Microsoft Exchange Server pour ses services de messagerie. Ces bases de données, qui

contiennent actuellement respectivement 11 Go et 15 Go de données, sont sauvegardées sur deux chargeurs automatiques HP StorageWorks DAT24.

L'architecture système d'ABC Le Cap comprend notamment le système SAP R/3 avec des bases de données Oracle. Trois serveurs HP T600 sont utilisés comme serveurs de base de données SAP. ABC Le Cap utilise des serveurs d'applications K260 SAP configurés en groupes d'application : Vente et distribution, Finances et Production. Ces serveurs d'applications ne présentent pas une grande disponibilité. L'environnement de sauvegarde actuel d'ABC Le Cap est décrit dans le tableau A-5 à la page A-24.

Figure A-5 Topologie de sauvegarde actuelle d'ABC Le Cap



Actuellement, à ABC Le Cap, les serveurs de base de données SAP sont sauvegardés à l'aide des utilitaires SAP BRBACKUP et SAP BRARCHIVE vers trois chargeurs automatiques HP StorageWorks DAT24. Chaque jour, les données sont copiées manuellement par les employés vers leurs serveurs respectifs. L'administrateur sauvegarde

séparément le serveur Microsoft Exchange et la base de données Microsoft SQL vers deux chargeurs automatiques HP StorageWorks DAT24.

Le même système est utilisé dans les bureaux de Durban et de Pretoria, à la différence près que ces succursales ne possèdent pas de système SAP. Les employés copient leurs données vers leurs serveurs respectifs. Chaque jour, les données sont sauvegardées vers un chargeur automatique HP StorageWorks DAT24.

Deux des serveurs d'ABC Pretoria contiennent plus de 500 000 fichiers chacun.

Les supports de sauvegarde sont marqués du nom du service, du nom du serveur et des dates de première et dernière sauvegardes qui y ont été effectuées. A la fin de chaque trimestre, les supports sont envoyés à un établissement central hors site pour y être stockés.

Problèmes rencontrés avec la solution actuelle

La solution de sauvegarde actuelle présente les inconvénients suivants :

- Il n'y a pas de solution de sauvegarde en ligne pour le serveur de base de données SAP.
- La solution de sauvegarde n'est pas centralisée.
- Les opérations de sauvegarde ne sont pas complètement automatisées.
- La gestion des supports requiert une intervention considérable du personnel.
- La récupération après sinistre est complexe.
- La durée des opérations de sauvegarde est plus longue que la durée autorisée.
- La solution de sauvegarde n'est pas adaptée au rythme de croissance élevé d'ABC.
- Il n'y a aucune génération de rapports ni notification sur les événements importants se rapportant à la sauvegarde.

Besoins relatifs à une stratégie de sauvegarde

Avant d'étudier les besoins relatifs à la stratégie de sauvegarde d'ABC, tenez compte des éléments énumérés à la section "Points à prendre en considération" à la page A-2.

Besoins

La section suivante décrit les besoins relatifs à la stratégie de sauvegarde d'ABC.

- Stratégie de l'organisation en matière de sauvegarde et de restauration :

  Selon la stratégie de l'entreprise pour l'archivage et le stockage de données, des sauvegardes hebdomadaires doivent être effectuées en **12 heures** et des sauvegardes incrémentales ou différentielles quotidiennes doivent être effectuées en **8 heures**.

- Temps d'indisponibilité maximum pour la récupération :

  Le temps d'indisponibilité autorisé a une incidence importante sur le choix des investissements en termes d'infrastructure réseau et de matériel dédié à la sauvegarde. Le tableau suivant donne, pour chaque type de données, le temps d'indisponibilité maximum acceptable pour la récupération des données, c'est-à-dire le temps pendant lequel des données spécifiques peuvent être indisponibles avant d'être récupérées à partir d'une sauvegarde.

Tableau A-6 Temps d'indisponibilité acceptable pour la récupération

Type de données	Temps d'indisponibilité maximum
Données commerciales de l'entreprise	6 heures
Données de ressources de l'entreprise	6 heures
Données de projet	1 jour
Données personnelles	2 jours

Le temps de récupération correspond essentiellement au temps nécessaire pour accéder aux supports et pour procéder à la restauration des données vers un disque.

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

  Le tableau A-7 à la page A-27 donne la durée de conservation nécessaire pour les différentes données. Cette durée a des répercussions sur le nombre de supports de sauvegarde requis.

Tableau A-7 Durée de conservation nécessaire pour les données

Type de données	Durée maximum de stockage des données
Données commerciales de l'entreprise	5 ans
Données de ressources de l'entreprise	5 ans
Données de projet	5 ans
Données personnelles	3 mois

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

  Les supports doivent être conservés dans la bibliothèque de bandes de la salle informatique. Toutes les données se trouvant sur le système de sauvegarde de l'entreprise doivent être archivées une fois par semaine par sauvegarde complète et tous les jours par sauvegarde incrémentale. Elles doivent être stockées dans les locaux d'une entreprise de sécurité.

- Quantité de données à sauvegarder :

  La quantité actuelle de données à sauvegarder est indiquée dans le tableau A-8 à la page A-27 :

Tableau A-8 Quantité de données à sauvegarder

Lieu	Données (en Go)
ABC Le Cap	100
ABC Pretoria	22
ABC Durban	16

Planification en vue de l'augmentation de la quantité de données

ABC prévoit que sa croissance annuelle sera de 15 à 20 %. La quantité de données à sauvegarder devrait donc évoluer en conséquence. Cette évolution aura des répercussions non seulement sur la durée des sauvegardes et sur les périphériques nécessaires à leur réalisation, mais également sur la taille de la base de données IDB.

Tableau A-9 Quantité de données à sauvegarder dans cinq ans

Lieu	Données (en Go)
ABC Le Cap	250
ABC Pretoria	55
ABC Durban	40

- A quelle fréquence sauvegarder les données ?

  Une sauvegarde complète de chaque type de données est effectuée une fois par semaine le vendredi, le samedi ou le dimanche. Des sauvegardes incrémentales de niveau un sont effectuées tous les jours ouvrables. Cependant, si une sauvegarde complète est effectuée le vendredi, les sauvegardes incrémentales de niveau un correspondantes sont effectuées les jours ouvrables et le samedi, mais pas le vendredi.

Solution proposée

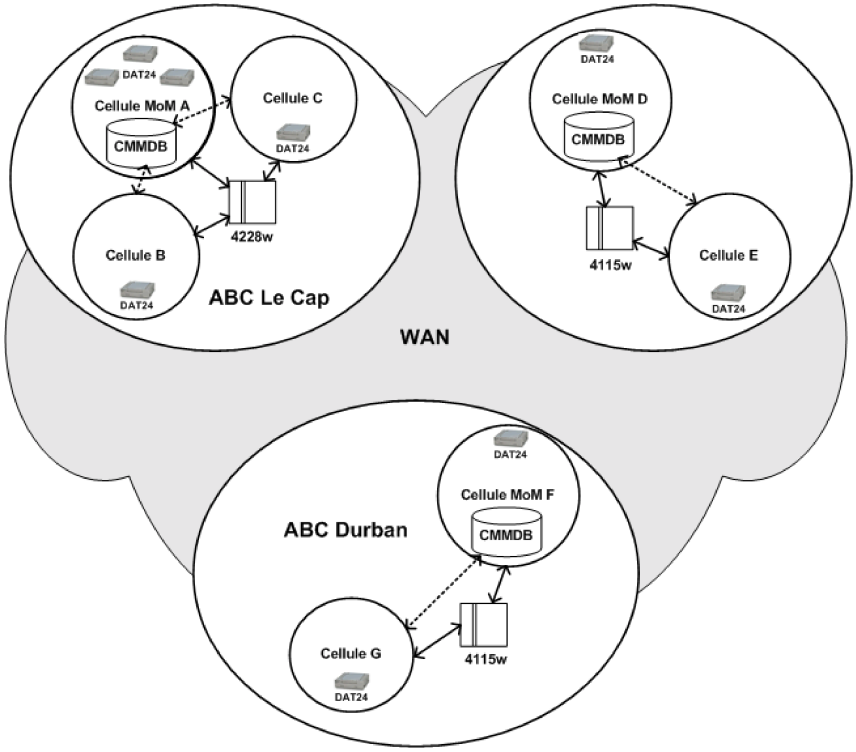
Compte tenu des défauts de la solution de sauvegarde actuelle, décrits à la section "Problèmes rencontrés avec la solution actuelle" à la page A-25, ABC projette de revoir la conception de son système de stockage de données.

Présentation générale de la solution

Chacun des trois services d'ABC Le Cap doit être configuré dans une cellule Manager-of-Managers (MoM). ABC Durban et ABC Pretoria doivent en outre être configurés en cellules MoM, comportant chacune deux cellules Data Protector.

Configurez la cellule A comme cellule MoM pour l'environnement d'ABC Le Cap, la cellule D comme cellule MoM pour celui d'ABC Pretoria et la cellule F comme cellule MoM pour celui d'ABC Durban. Cette configuration est représentée à la figure A-6 à la page A-29.

Figure A-6 Environnement d'entreprise d'ABC



Les systèmes Gestionnaire de cellule et Gestionnaire MoM des 7 cellules doivent être des systèmes Windows. Utilisez la base de données centralisée de gestion des supports (CMMDB) dans l'une des cellules de chaque environnement MoM, et des bases de données catalogues dans chacune des 7 cellules. La base de données centralisée de gestion des supports vous permet de partager des bibliothèques entre des cellules au sein de chaque environnement MoM.

Chacun des trois bureaux d'ABC doit disposer de sa propre bibliothèque. Utilisez la bibliothèque HP StorageWorks DLT 4228w pour l'environnement d'ABC Le Cap, et des bibliothèques HP StorageWorks DLT 4115w pour les environnements d'ABC Pretoria et d'ABC Durban.

Les trois cellules de l'environnement MoM d'ABC Le Cap doivent disposer chacune d'un serveur de base de données SAP. Ces serveurs se partagent la bibliothèque HP StorageWorks DLT 4228w. Les bases de données Microsoft SQL et Microsoft Exchange sont sauvegardées en local vers des chargeurs automatiques HP StorageWorks DAT24.

Les deux cellules de l'environnement MoM d'ABC Pretoria doivent également se partager une base de données centralisée de gestion des supports. Cette dernière doit être configurée sur le Gestionnaire MoM de la cellule D pour permettre le partage de la bibliothèque HP StorageWorks DLT 4115w entre les différentes cellules.

Les deux cellules de l'environnement MoM d'ABC Durban doivent également se partager une base de données centralisée de gestion des supports. Cette dernière doit être configurée sur le Gestionnaire MoM de la cellule F pour permettre le partage de la bibliothèque HP StorageWorks DLT 4115w entre les différentes cellules.

La solution proposée est décrite en détail ci-dessous :

Description détaillée de la solution proposée

- Configuration de la cellule

  Configurez les services en 7 cellules : 3 pour ABC Le Cap, 2 pour ABC Pretoria et 2 pour ABC Durban.

Pourquoi une configuration en 7 cellules ?

  — Les services d'ABC étant séparés géographiquement, il serait difficile de les gérer à partir d'une seule cellule. De plus, il y aurait un risque de problèmes réseau entre les systèmes. La configuration coïncide également avec le nombre de services, ce qui constitue un élément important en terme de sécurité. La taille de chaque cellule correspond également à celle recommandée de 30 à 50 systèmes client. Notez cependant que ce nombre dépend entre autres du nombre de fichiers et répertoires présents sur les différents systèmes client.

  Configurez ensuite l'environnement de chacun des trois bureaux comme environnement Manager-of-Managers. Ce dernier permet à l'utilisateur de gérer efficacement et en parfaite intégration plusieurs cellules à partir d'un point unique (gestion centralisée). Il permet également de configurer la base de données centralisée de gestion des supports (CMMDB) dans chaque environnement MoM.

Pourquoi utiliser la CMMDB ?

  — La base de données centralisée de gestion des supports (CMMDB) permet le partage de périphériques et de supports entre toutes les cellules d'un environnement MoM. Chacun des trois

environnements MoM d'ABC peut ainsi utiliser une bibliothèque unique, partagée par les systèmes client de toutes les cellules de l'environnement. L'utilisation d'une seule bibliothèque très volumineuse pour l'ensemble des données d'ABC ne serait guère pertinente, car cela nécessiterait pour la sauvegarde le transfert de grandes quantités de données via un WAN.

Utilisez une base de données catalogue dans chacune des 7 cellules. Les systèmes des cellules peuvent être ceux décrits dans le tableau A-10 à la page A-31 :

Tableau A-10 Configuration des cellules d'ABC

Environnement MoM	Cellule	Nb de serveurs Windows	Nb de clients Windows	Nb de serveurs UNIX	Nb de clients UNIX	Nb de SAP
ABC Le Cap	A*	3	24	2	7	1
	B	2	11	5	21	1
	C	2	20	4	12	1
ABC Pretoria	D*	4	33			
	E	1	6	5	32	
ABC Durban	F*	2	10	4	30	
	G	1	11	2	29	
Le nombre de SAP est le nombre de serveurs de base de données SAP.						
* correspond à une cellule MoM.						

Les systèmes Gestionnaire de cellule et Gestionnaire MoM des 7 cellules doivent être des systèmes Windows.

Pourquoi choisir le système Windows ?

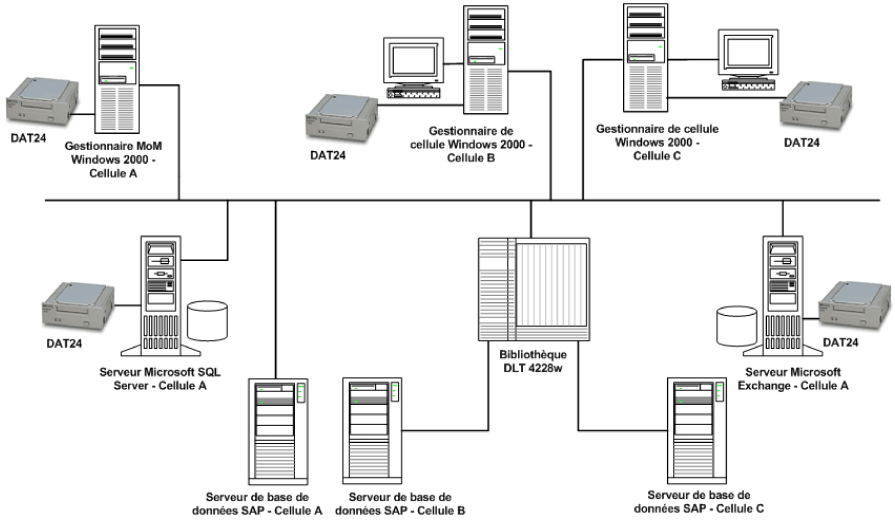
— Les systèmes Windows assurent la prise en charge de l'unicode natif et requièrent par conséquent une configuration moins poussée pour le traitemet des caractères internationaux dans les noms de fichiers.

Configurez la cellule A comme la cellule Manager-of-Managers de l'environnement d'ABC Le Cap, et importez le reste des cellules dans l'environnement MoM. Configurez une base de données centralisée de gestion des supports dans la cellule MoM A pour que la même bibliothèque puisse être partagée avec les cellules B et C. Partagez la

bibliothèque HP StorageWorks DLT 4228w pour l'environnement d'ABC Le Cap. Avec une capacité de 1,1 To au format compressé, cette bibliothèque devrait suffire pour les besoins prévus pour l'entreprise au cours des cinq années à venir.

Les trois cellules d'ABC Le Cap doivent être chacune dotées d'un serveur de base de données SAP. Ces serveurs se partagent la bibliothèque HP StorageWorks DLT 4228w. Les bases de données Microsoft SQL et Microsoft Exchange sont sauvegardées en local vers des chargeurs automatiques HP StorageWorks DAT24 existants. Chacune des cellules de l'environnement doit disposer de sa propre base de données catalogue. Vous trouverez une description de la configuration de l'environnement ABC Le Cap à la figure A-7 à la page A-32.

Figure A-7 Environnement de sauvegarde d'entreprise d'ABC Le Cap



Les deux cellules de l'environnement MoM d'ABC Pretoria doivent se partager une base de données centralisée de gestion des supports. Cette dernière doit être configurée sur le Gestionnaire MoM de la cellule D, afin de permettre le partage de la bibliothèque HP StorageWorks DLT 4115w entre les différentes cellules. Chacune des cellules de l'environnement doit disposer de sa propre base de données catalogue.

Les deux cellules de l'environnement MoM d'ABC Durban doivent également se partager une base de données centralisée de gestion des supports. Cette dernière doit être configurée sur le Gestionnaire MoM de la cellule F, et chacune des cellules de l'environnement doit avoir sa propre base de données catalogue.

Utilisez une bibliothèque HP StorageWorks DLT 4115w pour l'environnement d'ABC Pretoria et celui d'ABC Durban. Avec une capacité de 600 Go au format compressé, cette bibliothèque devrait suffire pour les besoins prévus pour chacun de ces environnements au cours des cinq années à venir.

Estimation de la taille de la base de données IDB

L'outil de planification de capacité de la base de données interne a été utilisé pour estimer la taille atteinte en une année par la base de données IDB de la cellule F. Cet outil se situe à l'emplacement suivant :

— Sur les systèmes Gestionnaire de cellule HP-UX et Solaris : `/opt/omni/doc/C/IDB_capacity_planning.xls`

— Sur le système Gestionnaire de cellule Windows : *<répertoire_Data_Protector>*`\docs\IDB_capacity_planning.xls`

Les paramètres d'entrée présentés à la figure A-8 à la page A-34 comprennent le nombre de fichiers dans l'environnement (2 millions), le facteur de croissance (1,2), la protection des données (260 semaines), la protection de catalogue (3 semaines), le nombre de sauvegardes complètes hebdomadaires (1) et le nombre de sauvegardes incrémentales hebdomadaires (5).

Figure A-8 Paramètres d'entrée

Description de l'environnement			
	Fichiers :	2	**millions**
	Fichiers par répertoire :	10	
	Volume de données :	16	**Go**
	Facteur de croissance :	1,20	
	Performances du périph. :	10,00	**Mo/s**
	Capacité du support :	70,00	**Go**
	Objets :	100	
	Modif. par sauv. incrément. :	10,00%	
Paramètres de sauvegarde			
	Périphériques simult. :	2	
	Taille segment données :	2048,00	**Mo**
	Niveau de journalisation :	Tout	
	Protection des données :	260	**semaines**
	Protection du catalogue :	3	**semaines**
	Sauv. complètes/semaine :	1	
	Sauv. incrémentielles/sem. :	5	
Param. du Gestionnaire de cellule	**Vitesse d'insertion :**	12	**millions/h**

Les résultats sont présentés à la figure A-9 à la page A-34. En une année, la base de données devrait croître pour atteindre environ 667,47 Mo.

Figure A-9 Résultats

Résultats/calculs			
	Taille de fichier moy. :	7,29	**Ko**
	Fichiers/segment :	269057,37	
	Taille de catalogue :	16,42	**Mo**
	Périphériques K :	2	
	Performances K :	85,48173913	**Go/h**
	Durée K :	0,19	**heure**
	Supports protégés :	133,7142857	
Estimation espace			
MMDB :		30,00	**Mo**
CDB :	**Fnames :**	207,00	**Mo**
	Overs :	57,13	**Mo**
	Mpos :	0,74	**Mo**
DCBF :		372,60	**Mo**
SMBF :		5,72	**Mo**
Total :		667,47	**Mo**

Vous pouvez également utiliser l'outil de planification de capacité de la base de données interne pour estimer la taille de la base de données IDB dans les environnements comportant des bases de données en ligne (Oracle, SAP R/3).

- Matériel
  - — Réseau

    Pour des performances optimales, l'ensemble des systèmes d'un même bureau d'ABC doit se trouver sur le même réseau local. Utilisez le réseau 100TX pour connecter tous les systèmes de chaque bureau, et le WAN pour connecter les cellules des trois bureaux d'ABC. Le réseau 100TX présente un taux de transfert de données de 10 Mo/s, ou 36 Go/h.

  - — Périphériques de sauvegarde

    Les périphériques de sauvegarde sont les suivants : une bibliothèque HP StorageWorks DLT 4228w pour ABC Le Cap et deux bibliothèques HP StorageWorks DLT 4115w pour ABC Pretoria et ABC Durban, ainsi que sept chargeurs automatiques HP StorageWorks DAT24 pour la sauvegarde des fichiers de configuration et de la base de données IDB dans toutes les cellules, et deux chargeurs automatiques HP StorageWorks DAT24 pour la sauvegarde des bases de données Microsoft SQL et Microsoft Exchange à ABC Le Cap. Actuellement, les serveurs Microsoft Exchange et Microsoft SQL hébergent respectivement 15 Go et 11 Go de données, tandis que le reste des données (100 Go - 15 Go - 11 Go = 74 Go) est sauvegardé à l'aide des serveurs de base de données SAP.

Pourquoi utiliser la bibliothèque HP StorageWorks DLT 4228w ?

La bibliothèque HP StorageWorks DLT 4228w dispose de deux lecteurs DLT4000 dotés de 28 emplacements. Elle présente une capacité totale de stockage compressé de 1,1 To, et un taux de transfert maximum de 6 Mo/s (2 x 3 Mo/s), soit 21 Go/h, avec compression de données. Il s'agit du taux sur lequel nous nous baserons pour la suite de cette section. Actuellement, la quantité totale de données à sauvegarder vers la bibliothèque HP StorageWorks DLT 4228w dans le cadre d'une sauvegarde complète, qu'il s'agisse d'une seule sauvegarde ou d'une sauvegarde échelonnée, est d'environ 74 Go. En supposant que la taille d'une sauvegarde incrémentale corresponde à environ 5 % de celle d'une sauvegarde complète, une génération de sauvegarde, c'est-à-dire une sauvegarde complète plus toutes les sauvegardes incrémentales qui en découlent, nécessite un espace de (74 + 74 x 5 % x 5) Go, soit **92,5 Go** dans la bibliothèque. D'ici cinq ans, cet espace nécessaire devrait augmenter pour atteindre environ 230 Go. La stratégie de

sauvegarde d'ABC nécessite la conservation de trois générations de sauvegarde de données. Un espace de 230 x 3 Go, soit 690 Go, est donc nécessaire dans la bibliothèque pour le stockage. La capacité de stockage (1,1 To) de la bibliothèque HP StorageWorks DLT 4228w est donc suffisante.

Au Cap, la bibliothèque est partagée entre les trois cellules. A Pretoria, elle est partagée entre les cellules D et E, et à Durban entre les cellules F et G. Ce type de configuration requiert l'utilisation de la base de données centralisée de gestion des supports Data Protector dans chacun des trois environnements MoM. Ces bases de données sont configurées sur le Gestionnaire MoM des cellules A, D et F.

Pourquoi utiliser la bibliothèque HP StorageWorks DLT 4115w ?

La bibliothèque HP StorageWorks DLT 4115w dispose d'un seul lecteur DLT4000 doté de 15 emplacements. Elle présente une capacité totale de stockage compressé de 600 Go et un taux de transfert maximum de 3 Mo/s, ou 10,5 Go/h, avec compression de données. Il s'agit du taux sur lequel nous nous baserons pour la suite de cette section. Actuellement, la quantité totale de données à sauvegarder à Pretoria vers la bibliothèque HP StorageWorks DLT 4115w dans le cadre d'une sauvegarde complète, qu'il s'agisse d'une seule sauvegarde ou d'une sauvegarde échelonnée, est d'environ 22 Go. En supposant que la taille d'une sauvegarde incrémentale corresponde à environ 5% de celle d'une sauvegarde complète, une génération de sauvegarde, c'est-à-dire une sauvegarde complète plus toutes les sauvegardes incrémentales qui en découlent, nécessite un espace de (22 + 22 x 5 % x 5) Go, soit **27,5 Go**, dans la bibliothèque. D'ici cinq ans, cet espace nécessaire devrait augmenter pour atteindre environ 68,75 Go. La stratégie de sauvegarde d'ABC nécessite la conservation de trois générations de sauvegarde de données. Un espace de 68,75 x 3 Go, soit 206,25 Go, est donc nécessaire dans la bibliothèque pour le stockage. La capacité de stockage (600 Go) de la bibliothèque HP StorageWorks DLT 4115w est donc suffisante.

Au Cap, des chargeurs automatiques HP StorageWorks DAT24 sont utilisés pour sauvegarder les serveurs Microsoft Exchange et Microsoft SQL ainsi que chacun des sept systèmes Gestionnaire de cellule des trois environnements MoM.

Pourquoi utiliser le chargeur automatique HP StorageWorks DAT24 ?

Le chargeur automatique HP StorageWorks DAT24 est doté de six cartouches de données de 24 Go. Elle présente une capacité totale de stockage compressé de 144 Go et un taux de transfert maximum de 2 Mo/s, ou 7 Go/h, avec compression de données. Il s'agit du taux sur lequel nous nous baserons pour la suite de cette section. Actuellement, la quantité totale de données à sauvegarder au Cap vers le chargeur automatique HP StorageWorks DAT24 (connecté au serveur Microsoft Exchange mentionné plus haut) est de 15 Go. En supposant que la taille d'une sauvegarde incrémentale corresponde à environ 5% de celle d'une sauvegarde complète, une génération de sauvegarde, c'est-à-dire une sauvegarde complète plus toutes les sauvegardes incrémentales qui en découlent, nécessite un espace de (15 + 15 x 5 % x 5) Go, soit **18,75 Go**. D'ici cinq ans, cet espace nécessaire devrait augmenter pour atteindre environ 47 Go. La stratégie de sauvegarde d'ABC nécessite la conservation de deux générations de sauvegarde de données. Un espace de 47 x 2 Go, soit **94 Go**, est donc nécessaire dans la bibliothèque pour le stockage. La capacité de stockage (144 Go) du chargeur automatique HP StorageWorks DAT24 est donc suffisante.

Combien de temps dure une sauvegarde complète ?

Au Cap, les serveurs de base de données des trois cellules contiennent environ 74 Go de données à sauvegarder vers une bibliothèque HP StorageWorks DLT 4228w. Cette dernière est dotée de deux lecteurs et présente un taux de transfert de données de 6 Mo/s (2 x 3 Mo/s), ou 21 Go/h. La sauvegarde des données dure par conséquent **5 heures maximum**. La quantité de données prévue dans cinq ans, soit 185 Go, devrait être sauvegardée en **9 à 10 heures**, ce qui reste inférieur aux 12 heures autorisées.

Les cellules D et E d'ABC Pretoria partagent une bibliothèque HP StorageWorks DLT 4115w. Cette dernière est dotée d'un seul lecteur et présente un taux de transfert de données de 3 Mo/s ou 10,5 Go/h. La quantité totale de données à sauvegarder dans ces cellules est d'environ 22 Go. La sauvegarde devrait donc prendre entre **2 et 3 heures**. La quantité de données prévue dans cinq ans, soit 55 Go, devrait être sauvegardée en **5 à 7 heures**, ce qui reste inférieur aux 12 heures autorisées.

De même, les 16 Go de données présents dans les cellules F et G d'ABC Durban doivent pouvoir être sauvegardés en **2 heures maximum**. La quantité de données prévue dans cinq ans, soit 40 Go, devrait être sauvegardée en **4 heures environ**, ce qui reste inférieur aux 12 heures autorisées.

La plus grande base de données catalogue Data Protector (1,3 Go) d'ABC Pretoria peut être sauvegardée en quelques minutes si aucune vérification d'intégrité n'est effectuée au préalable. Par défaut, Data Protector vérifie l'intégrité de la base de données avant que celle-ci ne soit sauvegardée. Cette vérification prend moins d'une heure pour une base de données de 1,3 Go. Par conséquent, les fichiers de configuration et la base de données IDB d'ABC Pretoria doivent pouvoir être sauvegardés en moins de **2 heures**.

- Pools de supports

  Les supports sont regroupés dans des pools pour être mieux suivis et contrôlés. Les pools de supports facilitent la gestion d'un grand nombre de supports, réduisant ainsi au minimum les efforts de gestion des administrateurs. Utilisez la structure de l'organisation et les critères des catégories de systèmes pour définir les pools de supports suivants :

Tableau A-11 Utilisation des pools de supports d'ABC

Nom du pool de supports	Lieu	Description
CT_SAP_Pool	Le Cap	Serveur de base de données SAP
CT_SQL_Pool	Le Cap	Serveur Microsoft SQL
CT_Exchange_Pool	Le Cap	Microsoft Exchange Server
CT_DB_Pool	Le Cap	IDB
P_DLT_Pool	Pretoria	Bibliothèque HP StorageWorks DLT 4115w
P_DAT_Pool	Pretoria	Chargeurs automatiques HP StorageWorks DAT24
P_DB_Pool	Pretoria	IDB

Tableau A-11 Utilisation des pools de supports d'ABC

Nom du pool de supports	Lieu	Description
D_DLT_Pool	Durban	Bibliothèque HP StorageWorks DLT 4115w
D_DAT_Pool	Durban	Chargeurs automatiques HP StorageWorks DAT24
D_DB_Pool	Durban	IDB

- Spécifications de sauvegarde

  Configurez les spécifications de sauvegarde comme suit :

  — DB_A...G :

  Spécifications de sauvegarde pour chacune des 7 bases de données IDB et les fichiers de configuration. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète par semaine et une sauvegarde incrémentale de niveau un tous les jours à 03:00, sauf le dimanche.

Pourquoi utiliser des sauvegardes incrémentales de niveau 1 ?

Pour restaurer les données les plus récentes, seuls deux jeux de supports sont nécessaires, l'un pour la dernière sauvegarde complète et l'autre pour la dernière sauvegarde incrémentale de niveau 1 précédant la restauration. Cela permet de simplifier et d'accélérer considérablement le processus de restauration. Lorsque des sauvegardes différentielles sont effectuées, le nombre de jeux de supports peut augmenter considérablement, rendant le processus de restauration plus complexe et plus lent.

Pour des raisons de sécurité, il est recommandé d'effectuer deux copies des fichiers de configuration et de la base de données IDB.

— SAP_A...C :

Spécification de sauvegarde pour les serveurs de base de données SAP respectivement dans les cellules A, B et C. Pour éviter les problèmes liés à une surcharge du réseau, à une surcharge des périphériques ou à la fenêtre temporelle, adoptez l'approche échelonnée telle qu'elle est décrite dans le tableau A-12 à la page A-40 :

Tableau A-12 Approche échelonnée pour ABC Le Cap

	Lun	Mar	Mer	Jeu	Ven	Sam	Dim
Cellule A	Incr1	Incr1	Incr1	Incr1	Complète	Incr1	
Cellule B	Incr1	Incr1	Incr1	Incr1	Incr1	Complète	
Cellule C	Incr1	Incr1	Incr1	Incr1	Incr1		Complète

— SERVERS_A...G :

Spécifications de sauvegarde des serveurs de l'entreprise pour la préparation à une récupération après sinistre. Cette spécification de sauvegarde est mise à jour à chaque installation d'un nouveau serveur ou mise à niveau d'un serveur existant. Planifiez les spécifications de sauvegarde de sorte que Data Protector exécute des sauvegardes complètes comme indiqué au tableau A-13 à la page A-41 et des sauvegardes incrémentales de niveau un tous les jours ouvrables.

— USERS_D...G :

Spécifications de sauvegarde pour les données utilisateur. Il s'agit de la sauvegarde de production principale à ABC Pretoria et ABC Durban. Planifiez la spécification de sauvegarde de sorte que Data Protector exécute une sauvegarde complète hebdomadaire chaque vendredi comme indiqué au tableau A-13 à la page A-41 et des sauvegardes incrémentales de niveau un tous les jours ouvrables. Cependant, si une sauvegarde complète est effectuée le vendredi, les sauvegardes incrémentales de niveau un correspondantes sont effectuées les jours ouvrables et le samedi, mais pas le vendredi.

La configuration de la spécification de sauvegarde est expliquée plus en détails dans le tableau A-13 à la page A-41.

Tableau A-13 Configuration de spécification de sauvegarde pour ABC

Nom	Cellule	Description	Jour de sauvegarde	Heure
DB_A	A	IDB	Samedi	03:00
DB_B	B	IDB	Samedi	03:00
DB_C	C	IDB	Samedi	03:00
SQL_A	A	Base de données Microsoft SQL	Vendredi	20:00
EXCHANGE_A	A	Base de données Microsoft Exchange	Vendredi	20:00
SAP_A	A	Serveur de base de données SAP	Vendredi	20:00
SAP_B	B	Serveur de base de données SAP	Samedi	20:00
SAP_C	C	Serveur de base de données SAP	Dimanche	20:00
SERVERS_A	A	Serveurs	Vendredi	23:00
SERVERS_B	B	Serveurs	Samedi	23:00
SERVERS_C	C	Serveurs	Dimanche	23:00
DB_D	D	IDB	Samedi	03:00
DB_E	E	IDB	Samedi	03:00
SERVERS_D	D	Serveurs	Vendredi	23:00
SERVERS_E	E	Serveurs	Samedi	23:00
USERS_D	D	Données utilisateur	Samedi	0:00
USERS_E	E	Données utilisateur	Dimanche	0:00

Tableau A-13 Configuration de spécification de sauvegarde pour ABC

Nom	Cellule	Description	Jour de sauvegarde	Heure
DB_F	F	IDB	Samedi	03:00
DB_G	G	IDB	Samedi	03:00
SERVERS_F	F	IDB	Vendredi	23:00
SERVERS_G	G	Serveurs	Samedi	23:00
USERS_F	F	Données utilisateur	Samedi	0:00
USERS_G	G	Données utilisateur	Dimanche	0:00

Options de sauvegarde

Utilisez les options de sauvegarde Data Protector par défaut. Définissez les options comme suit :

— Journaliser répertoires :

Cette option de sauvegarde de système de fichiers permet de s'assurer que seules les informations des répertoires sont stockées dans la base de données catalogue. La fonction de recherche est désactivée pendant la restauration et vous pouvez parcourir uniquement les répertoires. Utilisez cette option pour sauvegarder les deux serveurs de la cellule D contenant plus de 500 000 fichiers chacun. Sinon, la taille de la base de données catalogue Data Protector risque d'augmenter considérablement.

— Protection :

Les données doivent pouvoir être accessibles pendant trois semaines. Une sauvegarde complète devant avoir lieu chaque semaine, choisissez une protection de catalogue de 27 jours (3 semaines x 7 jours + 6 jours = 27 jours).

Choisissez une protection de données de 5 ans pour toutes les spécifications de sauvegarde, sauf Exchange_A qui sert à la sauvegarde du courrier personnel. Pour cette spécification de sauvegarde, optez pour une protection de données de 3 mois.

— Simultanéité :

Réglez sur 5 le nombre d'Agents de disque pouvant écrire simultanément des données dans la bibliothèque. Vous améliorerez ainsi les performances de sauvegarde.

— Pool de supports :

Sélectionnez les pools de supports et les supports appropriés pour la sauvegarde.

- Génération de rapports et notification

  Des notifications envoyées par e-mail aux administrateurs de sauvegarde sont définies pour les demandes de montage, en cas d'espace insuffisant dans la base de données, en cas d'erreur de périphérique et à la fin des sessions pour toutes les spécifications de sauvegarde. Eventuellement, des notifications par e-mail ou message de diffusion sont définies pour les utilisateurs finaux souhaitant être informés de la réussite des sauvegardes de leurs systèmes.

  Pour permettre à tous les utilisateurs de connaître facilement l'état de leurs sauvegardes, définissez comme suit les informations de sauvegarde client sur la page d'accueil de l'entreprise :

  1. Configurez un groupe de rapports avec un rapport sur la sauvegarde client pour chaque client. Le rapport doit être enregistré dans le fichier au format HTML.
  2. Planifiez le groupe de rapports.
  3. Reliez les fichiers contenant les rapports à la page d'accueil de l'entreprise.

- Mise au coffre

  La mise au coffre consiste à stocker des supports en lieu sûr pendant une période déterminée.

  Des supports sont déplacés une fois par semaine vers le coffre, et remplacés par de nouveaux supports dans les bibliothèques HP StorageWorks DLT 4228w et 4115w, et les chargeurs automatiques HP StorageWorks DAT24. Toutes les actions, hormis le déplacement de supports vers le coffre, sont exécutées par la solution logicielle, notamment les requêtes effectuées en interne dans la base de données pour éviter à l'administrateur d'avoir à rechercher les supports devant être éjectés.

Effectuez le suivi des supports déplacés vers un coffre. Cette opération est utile lorsque vous souhaitez restaurer des données à partir de sauvegardes réalisées sur un support déplacé vers le coffre. Data Protector vous permet d'effectuer les tâches de mise au coffre suivantes :

— Génération de rapports sur les supports stockés à un endroit spécifique et dont la protection de données expire à une date déterminée ;

— Génération de rapports sur les supports utilisés pour une sauvegarde au cours d'une période donnée ;

— Affichage d'une liste de spécifications de sauvegarde ayant utilisé des supports spécifiques lors de la sauvegarde ;

— Affichage d'une liste de supports nécessaires pour les opérations de restauration et des emplacements physiques où sont stockés ces supports ;

— Filtrage des supports à partir de l'affichage des supports selon des critères spécifiques (affichage des supports dont la protection a expiré, par exemple).

- Restauration

  — Restaurer par requête

  Les demandes de restauration par requête sont envoyées à l'administrateur. Si la dernière sauvegarde des fichiers date de moins de 3 semaines avant l'envoi de la requête, l'administrateur peut utiliser l'option Restaurer par requête pour sélectionner les fichiers et répertoires à restaurer selon des critères déterminés. Il choisit ensuite l'option Ecraser pour remplacer les fichiers et répertoires du disque par les versions figurant sur le support.

  — Restaurer système de fichiers

  Les demandes de restauration de systèmes de fichiers entiers sont envoyées à l'administrateur. Si la dernière sauvegarde des fichiers date de moins de 3 semaines avant l'envoi de la demande, l'administrateur peut sélectionner l'objet à restaurer et utiliser l'option Restaurer dans.

Les objets sont alors restaurés avec la même structure de répertoires dans un répertoire sélectionné. Servez-vous d'un utilitaire Windows ou UNIX pour comparer les objets restaurés aux objets sauvegardés.

— Restaurer à partir d'un coffre :

Pour restaurer des données à partir d'un coffre, sauvegardées par exemple 3 ans auparavant, envoyez une demande à l'administrateur, qui effectue alors les opérations suivantes :

1. Il identifie les supports nécessaires à la restauration.
2. Il déplace les supports du coffre vers la bibliothèque HP StorageWorks DLT 4228w, la bibliothèque HP StorageWorks DLT 4115w ou vers un autre périphérique, puis les analyse.
3. Si les supports ne se trouvent pas dans la base de données catalogue Data Protector, il sélectionne l'objet spécifique à restaurer à l'aide de l'option Lister depuis supports.
4. Il effectue la restauration.

B Informations supplémentaires

Dans cette annexe

La présente annexe fournit des informations supplémentaires sur certains aspects des concepts de Data Protector, notamment la génération de sauvegardes, des exemples de copie automatisée des supports et l'internationalisation.

Générations de sauvegarde

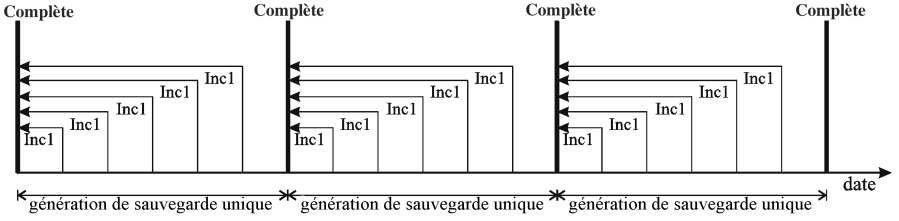
Data Protector propose un modèle de protection associé à l'heure / la date. Il est facile d'établir une correspondance entre un modèle de sauvegarde basé sur les générations et le modèle basé sur l'heure, à condition que les sauvegardes soient effectuées régulièrement.

Qu'est-ce qu'une génération de sauvegarde ?

Une génération de sauvegarde (voir figure B-1 à la page B-3) est constituée d'une sauvegarde complète ainsi que de toutes les sauvegardes incrémentales basées sur cette sauvegarde complète. Lorsque la sauvegarde complète suivante est effectuée, une nouvelle génération de sauvegarde est créée.

Les générations de sauvegarde permettent de savoir combien de versions complètes de données sauvegardées ont été réalisées. Pour pouvoir effectuer une restauration de l'état à un instant donné, vous devez disposer d'au moins une génération de sauvegarde (c'est-à-dire une sauvegarde complète ainsi que toutes les sauvegardes incrémentales jusqu'à cet instant). Conservez plusieurs générations de sauvegarde (trois par exemple), selon la réglementation de protection des données adoptée par votre entreprise.

Figure B-1 **Générations de sauvegarde**



Pour configurer Data Protector afin qu'il conserve automatiquement le nombre souhaité de générations de sauvegarde, choisissez les durées de protection des données et de catalogue adéquates et programmez les sauvegardes sans surveillance (complètes et incrémentales).

Pour conserver par exemple trois générations de sauvegarde alors que vous effectuez une sauvegarde complète par semaine et une sauvegarde incrémentale remise à niveau par jour, définissez la protection des données à 7 x 3 + 6 = 27 jours. Une génération de sauvegarde est

constituée d'une sauvegarde complète ainsi que de toutes les sauvegardes incrémentales effectuées jusqu'à la prochaine sauvegarde complète : par conséquent, le chiffre six dans la formule représente les sauvegardes incrémentales effectuées avant la génération de sauvegarde suivante (soit la quatrième) et appartenant à la troisième génération de sauvegarde.

Vous pouvez mettre en place une rotation automatique des supports (pour les supports dont le temps de protection a expiré) avec une politique d'utilisation des pools appropriée. Pour plus d'informations, reportez-vous à la section “Mise en œuvre d'une stratégie de rotation des supports” à la page 146.

Exemples de copie automatisée des supports

Une fois une sauvegarde terminée, vous pouvez utiliser la fonction de copie automatisée des supports pour copier les supports, puis placer les originaux ou les copies dans un coffre hors site. Selon les périphériques disponibles, vous pouvez utiliser la copie de supports après sauvegarde ou la copie de supports programmée.

Il convient de prendre en considération les éléments suivants :

- Il est recommandé d'effectuer toutes les sauvegardes avant de copier les supports.
- Pendant l'opération de copie, les supports en cours de copie ne sont pas disponibles pour la restauration.
- Vous pouvez uniquement copier le support dans son intégralité : il est impossible de copier des objets spécifiques.
- Une fois la copie effectuée, les supports source qui ont été copiés et les copies sont marqués comme sans possibilité d'ajout, ce qui signifie que vous ne pouvez pas ajouter de nouvelles sauvegardes à ces supports.
- Dans le cas de la copie de supports programmée, les périphériques et les supports nécessaires doivent être disponibles à l'heure prévue ; si ce n'est pas le cas, l'opération de copie est abandonnée.

Exemple 1 : copie automatisée des supports de sauvegardes de systèmes de fichiers

Votre entreprise dispose d'un environnement MoM doté de deux cellules contenant chacune 150 systèmes informatiques (serveurs et stations de travail). Chaque système dispose en moyenne de 10 Go de données, soit au total 3000 Go à sauvegarder.

Vous souhaitez disposer de sauvegardes Incr1 quotidiennes des données, de sauvegardes hebdomadaires complètes et de sauvegardes mensuelles complètes à des fins d'archivage. Les sauvegardes doivent être effectuées en dehors des heures ouvrées de l'entreprise, ce qui signifie qu'elles peuvent débuter après 17:00 et doivent s'achever avant 8:00 le lendemain matin ; elles peuvent également être effectuées en fin de semaine.

Vous décidez de faire des copies des supports de sauvegarde, qui resteront sur site à des fins de restauration, et de déplacer les originaux vers un coffre hors site par mesure de sécurité. Les supports doivent être copiés après la fin des sauvegardes. Pour ce faire, vous utiliserez la copie automatisée des supports.

Vous utilisez une bibliothèque de bandes HP StorageWorks 6/60 dotée de 6 lecteurs LTO et des supports LTO Ultrium 1. En fonction de votre expérience passée, vous estimez que le transfert des données s'effectue au rythme d'environ 80 Go par heure ; la capacité moyenne d'un support est de 153 Go.

Après l'opération de copie des supports, les supports source et cible sont sans possibilité d'ajout. Par conséquent, il peut être préférable de réduire le nombre de supports requis pour la sauvegarde. Il est recommandé de commencer avec des supports vierges et d'utiliser pleinement leur capacité. Pour ce faire, vous pouvez créer des spécifications de sauvegarde en affectant un seul périphérique à cette opération. Ainsi, tout nouveau support ne sera utilisé qu'une fois que le support en cours sera plein. Toutefois, la durée de la sauvegarde est alors plus longue que si vous utilisez plusieurs supports en parallèle.

Vous décidez de créer 4 spécifications de sauvegarde. Pour économiser l'espace sur les supports, les données sont divisées entre les spécifications de sauvegarde de manière à utiliser le nombre minimum possible de supports. Un seul périphérique est affecté à chaque sauvegarde.

La copie automatisée des supports est effectuée après la fin de la sauvegarde. Vous pouvez utiliser tous les périphériques disponibles pour cette opération. Cela signifie que 3 périphériques seront respectivement utilisés pour les supports source et pour les supports cible.

On estime que la durée de la copie des supports sera environ équivalente à la durée de la sauvegarde.

Sauvegarde Incr1

Configuration des sauvegardes

Vous planifiez des sauvegardes Incr1 chaque jour du lundi au jeudi à 18:00. La protection des données est définie sur 4 semaines. En supposant que 30 % des données sont modifiées chaque jour, cela représente 900 Go de données à sauvegarder. Les données sont divisées entre les spécifications de sauvegarde de la manière suivante :

- Spécif. de sauv. 1 (Lecteur 1) - 300 Go

- Spécif. de sauv. 2 (Lecteur 2) - 300 Go
- Spécif. de sauv. 3 (Lecteur 3) - 150 Go
- Spécif. de sauv. 4 (Lecteur 4) - 150 Go

Spécif. de sauv. 1 et Spécif. de sauv. 2 requièrent chacune 2 supports et la sauvegarde dure environ 4 heures. Spécif. de sauv. 3 et Spécif. de sauv. 4 requièrent chacune 1 support et la sauvegarde dure environ 2 heures.

Configuration de la copie automatisée des supports

La copie automatisée des supports de chaque sauvegarde commence une fois la sauvegarde terminée. Vous avez 6 supports à copier et vous pouvez utiliser tous les lecteurs de la bibliothèque pour cette opération, dès que les périphériques sont disponibles.

Vous pouvez utiliser la copie des supports après sauvegarde pour copier les supports utilisés pour les opérations Spécif. de sauv. 1 et Spécif. de sauv. 2, dans la mesure où deux lecteurs (lecteur 5 et lecteur 6) sont libres ; par conséquent, vous n'avez pas à vous préoccuper de la disponibilité des périphériques.

Vous configurez la copie des supports après sauvegarde pour Spécif. de sauv. 1 et sélectionnez le lecteur 1 comme périphérique source et le lecteur 6 comme périphérique cible. Vous définissez la même protection des données que pour l'original et spécifiez l'emplacement des supports (par exemple, Etagère 1).

Vous configurez également la copie des supports après sauvegarde pour Spécif. de sauv. 2 et sélectionnez le lecteur 2 comme périphérique source et le lecteur 5 comme périphérique cible. Vous définissez la même protection des données que pour l'original et spécifiez l'emplacement des supports.

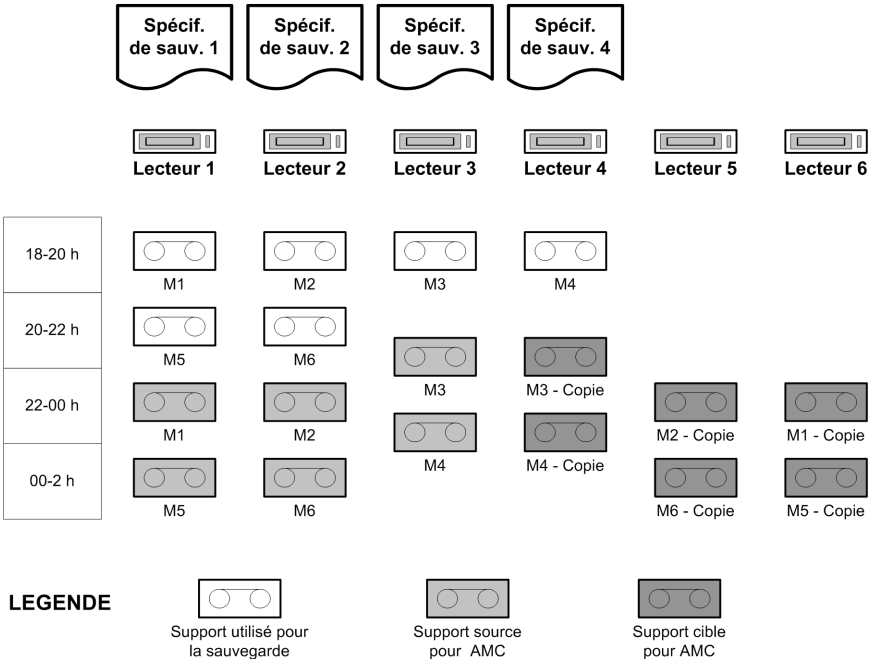
Vous utilisez la copie programmée des supports pour copier les supports utilisés par Spécif. de sauv. 3 et Spécif. de sauv. 4, car vous utiliserez le lecteur 3 et le lecteur 4 pour l'opération de copie et vous devez attendre la fin des deux sauvegardes. Notez que si les périphériques ne sont pas disponibles au moment où la copie des supports est programmée, l'opération échouera. C'est la raison pour laquelle il est recommandé d'ajouter une certaine marge à la durée estimée de la sauvegarde lors de la programmation de l'opération de copie automatisée des supports qui utilisera les mêmes périphériques.

Vous programmez l'opération de copie des supports une heure après l'heure de fin estimée de la sauvegarde et sélectionnez Spécif. de sauv. 3 et Spécif. de sauv. 4 pour les copier ; vous sélectionnez ensuite le lecteur

3 comme périphérique source et le lecteur 4 comme périphérique cible. Vous définissez la même protection des données que pour l'original et spécifiez l'emplacement des supports.

Pour obtenir une représentation graphique de la sauvegarde Incr1 et de la copie automatisée des supports, reportez-vous à la figure B-2 à la page B-8.

Figure B-2 Sauvegarde Incr1 et copie automatisée des supports



Sauvegarde complète

Configuration des sauvegardes

Vous programmez la sauvegarde hebdomadaire complète pour le vendredi à 18:00. La protection des données est définie sur 8 semaines. Vous avez 3000 Go de données à sauvegarder. Les données sont divisées entre les spécifications de sauvegarde de la manière suivante :

- Spécif. de sauv. 1 (Lecteur 1) - 1000 Go
- Spécif. de sauv. 2 (Lecteur 2) - 1000 Go

- Spécif. de sauv. 3 (Lecteur 3) - 500 Go
- Spécif. de sauv. 4 (Lecteur 4) - 500 Go

Spécif. de sauv. 1 et Spécif. de sauv. 2 requièrent chacune 7 supports ; Spécif. de sauv. 3 et Spécif. de sauv. 4 requièrent chacune 4 supports. La sauvegarde s'effectue en 14 heures environ.

Configuration de la copie automatisée de supports

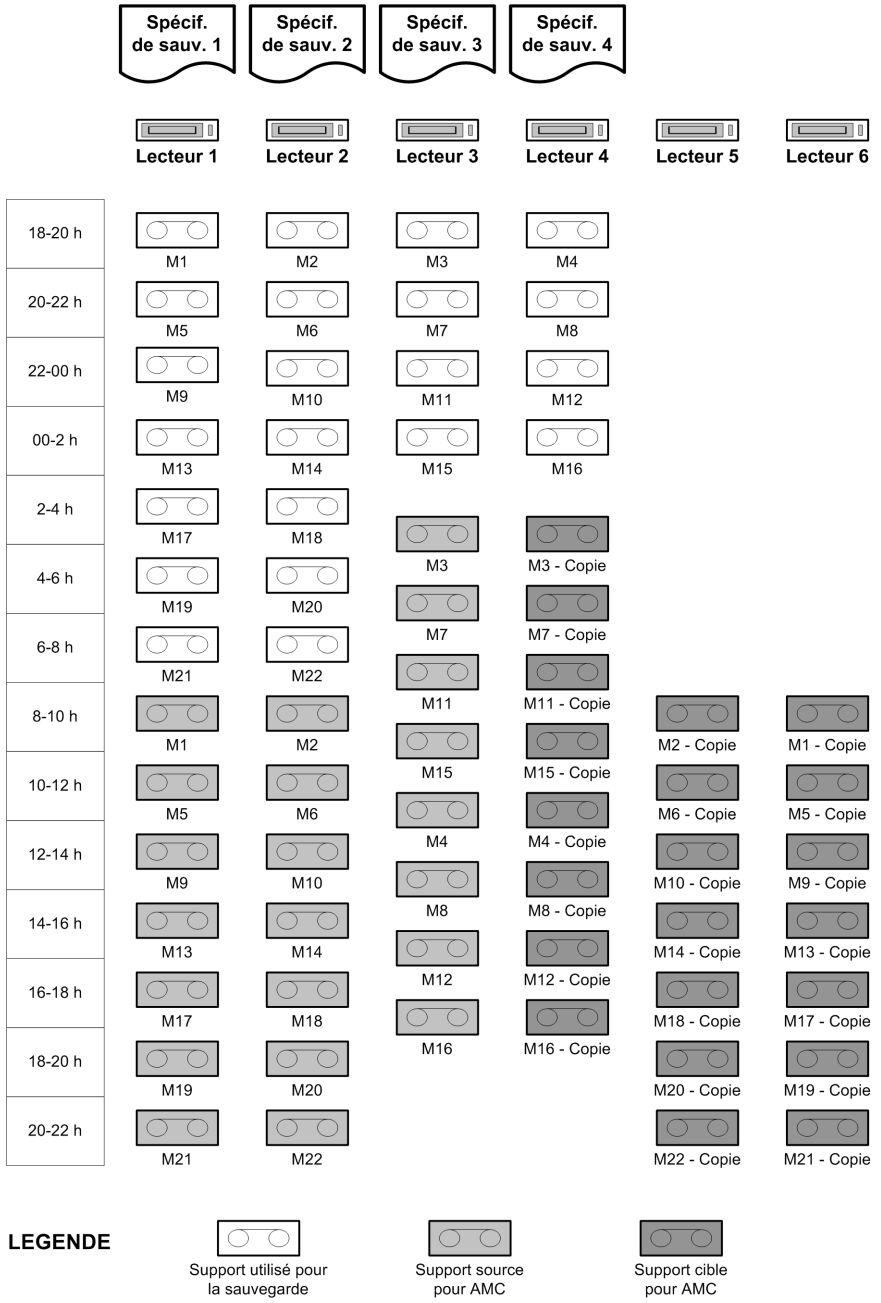
La copie automatisée des supports de chaque sauvegarde commence une fois la sauvegarde terminée. Vous avez 22 supports à copier et tous les périphériques sont utilisés dès qu'ils sont disponibles.

Encore une fois, vous utilisez la copie de supports après sauvegarde pour copier les supports utilisés avec Spécif. de sauv. 1 et Spécif. de sauv. 2, et la copie programmée pour les supports utilisés pour Spécif. de sauv. 3 et Spécif. de sauv. 4.

Les périphériques et les paramètres de protection des données sont identiques à ceux qui ont été utilisés pour la copie de la sauvegarde Incr1. La copie programmée des supports commence une heure après l'heure de fin estimée de la sauvegarde.

Pour obtenir une représentation graphique de la sauvegarde complète et de la copie automatisée des supports, reportez-vous à la figure B-3 à la page B-10.

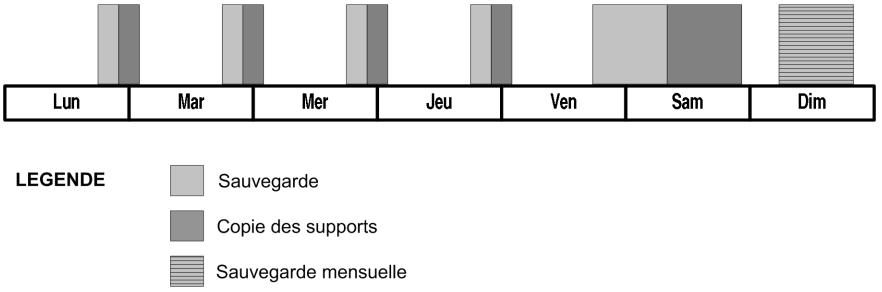
Figure B-3 **Sauvegarde complète et copie automatisée des supports**



Vous programmez votre sauvegarde mensuelle complète pour le dimanche à 6:00. Cette sauvegarde étant destinée à l'archivage, elle n'est pas habituellement copiée.

La figure B-4 à la page B-11 présente un aperçu général des périodes d'occupation des périphériques. Notez qu'il s'agit d'une présentation grossière, de sorte que le graphique ne tient pas compte du chevauchement partiel de certaines sessions de sauvegarde et de copie.

Figure B-4 Présentation des sessions de sauvegarde et de copie automatisée des supports



Exemple 2 : copie automatisée des supports de sauvegardes de base de données Oracle

Votre entreprise dispose d'une base de données Oracle de 500 Go. Vous souhaitez effectuer quotidiennement une sauvegarde complète de la base de données. La sauvegarde doit être effectuée en dehors des heures ouvrées de l'entreprise, ce qui signifie qu'elle peut débuter après 17:00 et doit s'achever avant 8:00 le lendemain matin ; elle peut également être effectuée en fin de semaine.

Vous utilisez la copie automatisée pour copier les supports de sauvegarde ; ces copies resteront sur le site à des fins de restauration. Les originaux seront déplacés vers un coffre hors site par mesure de sécurité. Les supports doivent être copiés après la fin de la sauvegarde. Pour ce faire, vous utiliserez la copie des supports après sauvegarde.

Vous utilisez une bibliothèque de bandes HP StorageWorks 10/700 dotée de 10 lecteurs LTO et des supports LTO Ultrium 1. En fonction de votre expérience passée, vous estimez que le transfert des données s'effectue au rythme d'environ 80 Go par heure ; la capacité moyenne d'un support est de 153 Go.

Après l'opération de copie des supports, les supports utilisés pour la sauvegarde et la copie des supports sont sans possibilité d'ajout ; par conséquent, il peut être préférable d'utiliser autant d'espace que possible sur la bande. Par ailleurs, vous souhaitez que la sauvegarde se termine dès que possible. Vous utilisez 4 périphériques pour la sauvegarde. Il est recommandé de commencer avec des supports vierges et d'utiliser pleinement leur capacité.

La copie automatisée des supports commence après la fin de la sauvegarde. Vous avez 4 supports à copier et affectez par conséquent 8 périphériques à cette opération. Cela signifie que 4 périphériques seront respectivement utilisés pour les supports source et pour les supports cible.

On estime que la durée de la copie des supports sera environ équivalente à la durée de la sauvegarde.

Sauvegarde complète

Configuration des sauvegardes

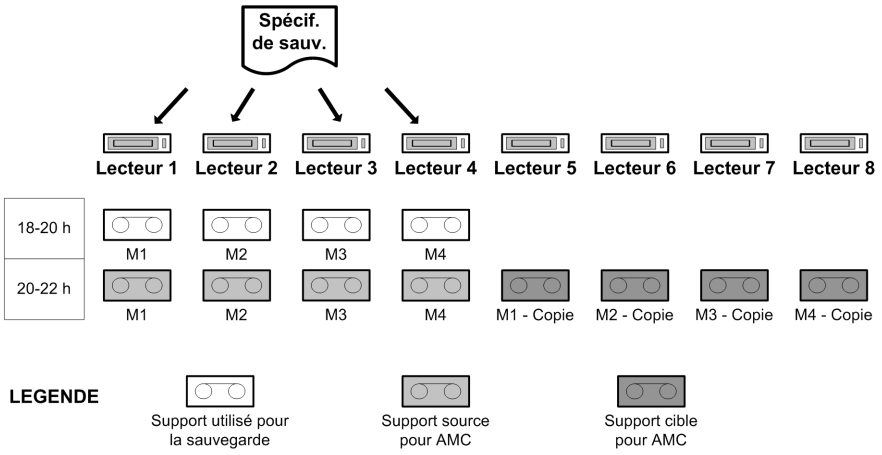
Vous programmez la sauvegarde complète quotidienne chaque jour du lundi au vendredi à 18:00. La protection des données est définie sur 4 semaines. Vous avez 500 Go de données à sauvegarder. Vous utilisez les lecteurs 1, 2, 3 et 4. La sauvegarde utilise 4 supports et s'effectue en 2 heures environ.

Configuration de la copie automatisée de supports

Vous utilisez la copie des supports après sauvegarde car vous disposez d'un nombre suffisant de périphériques. Vous spécifiez les lecteurs 1, 2, 3 et 4 en tant que périphériques source et les lecteurs 5, 6, 7 et 8 en tant que périphériques cible. Vous définissez la même protection des données que pour l'original et spécifiez l'emplacement des supports.

Pour obtenir une représentation graphique de la sauvegarde complète de la base de données et de la copie automatisée des supports, reportez-vous à la figure B-5 à la page B-13.

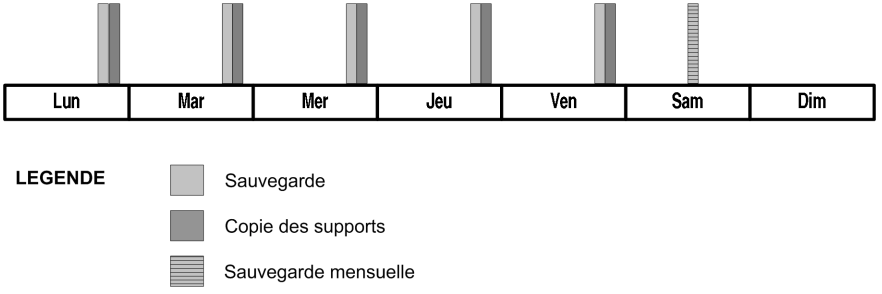
Figure B-5 **Sauvegarde complète de la base de données et copie automatisée des supports**



Vous programmez votre sauvegarde complète mensuelle pour le samedi à midi. Cette sauvegarde étant destinée à l'archivage, elle n'est pas habituellement copiée.

La figure B-6 à la page B-13 présente un aperçu général des périodes d'occupation des périphériques.

Figure B-6 **Présentation des sessions de sauvegarde et de copie automatisée des supports**



Internationalisation

L'internationalisation consiste à développer et à mettre en œuvre un logiciel de sorte que le produit interagisse avec la langue maternelle de l'utilisateur, et conformément aux paramètres locaux de l'utilisateur (devise, heure, date, nombres et autres formats). L'utilisateur peut ainsi saisir les données de texte dans sa langue et les afficher correctement. L'internationalisation, dans le cadre du développement d'un logiciel, est la procédure qui permet de mettre en œuvre un seul logiciel avec une source et un binaire uniques. Ce sont les textes proprement dits (indépendants des binaires) qui sont traduits afin de localiser le logiciel en plusieurs langues. L'internationalisation est donc un processus destiné à permettre la localisation. Data Protector est un produit internationalisé dont l'interface utilisateur est proposée en plusieurs langues.

Localisation

La localisation consiste à adapter un produit ou un service à une langue et à une culture particulières. Il s'agit notamment de proposer des écrans, une aide en ligne, des messages d'erreurs, des manuels, etc. localisés.

Au lieu d'envoyer les chaînes de message proprement dites, Data Protector envoie les ID des chaînes provenant des agents au Gestionnaire de cellule. Ensuite, le Gestionnaire de cellule transfère les chaînes à l'interface, laquelle affiche les messages dans le format de langue approprié. Notez que les noms des répertoires et des fichiers ne sont pas indexés. Ils sont transmis sous forme de chaînes de texte et présentés tels quels dans l'interface. Les implications de cette démarche sont traitées dans la section "Gestion des noms de fichier" à la page B-15.

Data Protector est localisé en plusieurs langues. Pour plus d'informations sur les langues disponibles, reportez-vous aux *Notes de publication du logiciel HP OpenView Storage Data Protector* ou adressez-vous à votre fournisseur ou à votre service de vente HP.

Gestion des noms de fichier

Le traitement des noms de fichiers dans un environnement hétérogène (différents systèmes d'exploitation et différents paramètres locaux dans une même cellule) est un défi important. Data Protector traite les noms selon les différents paramètres locaux (tels que la langue, la zone géographique et les jeux de caractères) utilisés sur le système lors de la création des noms de fichiers. Les noms de fichiers qui ont été sauvegardés à l'aide de certains paramètres locaux puis affichés ou restaurés à l'aide d'autres paramètres locaux, requièrent une configuration spécifique pour s'afficher correctement.

Quelques explications

Les différents fournisseurs de plates-formes utilisent une grande diversité de représentations de caractères ou de normes d'encodage des caractères (telles qu'ISO 8859-1, Shift-JIS, EUC, Code Page 932 et Unicode) pour prendre en charge les différents jeux de langues. Ces codages entrent en conflit les uns avec les autres - deux codages peuvent utiliser la même valeur pour deux caractères *différents* ou bien différentes valeurs pour le *même* caractère. Après la création d'un nom de fichier, aucun jeu de codes ayant été utilisé n'est indiqué. Il se peut que les noms de fichiers transmis entre plusieurs systèmes au moyen de différents codages ne s'affichent pas dans l'interface graphique.

La transmission de données entre différentes plates-formes n'est pas problématique si toutes les plates-formes utilisent une implémentation d'Unicode (UTF-16 sous Windows et UTF-xx sur d'autres plates-formes) hébergeant tous les caractères.

Malheureusement, l'implémentation UTF-xx d'Unicode n'est pas une norme sur les systèmes UNIX. Les composants de l'application peuvent être répartis sur plusieurs systèmes et plates-formes, tels que Windows XP Professionnel, Windows 2000, HP-UX, Solaris et AIX. Les données figurant sur ces différentes plates-formes doivent être sauvegardées et restaurées. A défaut de pouvoir compenser l'absence d'une représentation commune à l'échelle du secteur pour les langues et les jeux de caractères, Data Protector atténue son impact pour l'utilisateur.

Exemple

Avec certaines configurations dans des environnements hétérogènes, les noms de fichiers peuvent apparaître altérés dans l'interface graphique. Lors de l'utilisation de Data Protector, il est possible par exemple de sauvegarder des fichiers sur une plate-forme HP-UX sur laquelle l'Agent de disque est en cours d'exécution, et d'afficher ces fichiers dans

l'interface graphique Data Protector qui fonctionne sous Windows. A moins que des jeux de codes identiques ne soient utilisés sur les deux plates-formes, il se peut que les noms de fichiers ne s'affichent pas correctement. Cela est dû au fait que la même valeur de caractère peut avoir une signification et une apparence différentes selon le jeu de codage utilisé.

Exemple d'incompatibilité avec UNIX

Trois utilisateurs travaillant sous un système Solaris sur lequel Data Protector n'est pas installé et utilisant des jeux de caractères différents créent des fichiers sous le même système de fichiers, hors plage de caractères ASCII. Si les utilisateurs se servent alors de la commande `ls` pour afficher les fichiers qu'ils ont créés ainsi que ceux créés par les autres utilisateurs, la situation suivante apparaît :

- Chaque utilisateur voit ses propres noms de fichier correctement affichés.
- Chaque utilisateur voit les noms de fichier des autres utilisateurs comme altérés. Les noms de fichier altérés peuvent apparaître différemment sous les divers systèmes.

Les noms de fichier corrompus ont été créés avec un jeu de codage différent de celui utilisé pour exécuter la commande `ls`. Ils ne sont pas dotés d'une balise indiquant le jeu de codage utilisé pour leur création. Ce phénomène se produit sur les systèmes utilisant des afficheurs de systèmes de fichiers natifs, par exemple `ls` dans la fenêtre du terminal.

Gestion des noms de fichier lors d'une sauvegarde

Data Protector lit les noms de fichier à l'aide de l'Agent de disque (lequel s'exécute sur le client devant être sauvegardé) et enregistre une copie originale sur un support. Si l'option `log filename` est activée pour la sauvegarde, les noms de fichier sont également convertis dans un jeu de codage "interne" et reliés à la base de données IDB.

Exploration des noms de fichier

Il est possible de sélectionner les fichiers via l'interface Data Protector avant la restauration. Pour cela, il suffit d'afficher les noms de fichiers dans la base de données IDB sur le système exécutant l'interface graphique. Data Protector propose plusieurs codages pour visualiser les noms de fichiers apparaissant dans son interface graphique. Lorsqu'un codage de caractères spécifique est utilisé, Data Protector l'utilise pour afficher les caractères dans les noms de fichiers.

Pour afficher correctement des noms de fichiers, sélectionnez le codage de caractères utilisé sur le système sur lequel les fichiers ont été créés. Dans le cas contraire, les noms de fichiers apparaissent corrompus dans l'interface graphique de Data Protector.

Les noms de fichiers corrompus peuvent être restaurés sur la plate-forme sur laquelle les sauvegardes ont été effectuées.

Reportez-vous au mot clé de l'index de l'aide en ligne `internationalization` pour obtenir une liste de configurations indiquant les restrictions en matière d'exploration des noms de fichiers.

Gestion des noms de fichier lors d'une restauration

Les fichiers sont généralement restaurés sur la plate-forme utilisée pour les sauvegardes. La procédure se déroule comme suit :

- Vous devez sélectionner les fichiers à restaurer dans l'interface.
- Data Protector recherche sur la bande les données correspondantes et les restaure.
- Les noms de fichier originaux (c'est-à-dire les copies originales provenant de la bande) sont restaurés.

Glossaire

AC *(terme spécifique à HP StorageWorks Disk Array XP)*
L'accès continu XP (Continuous Access) permet à l'utilisateur de créer et de conserver des copies distantes de LDEV HP StorageWorks Disk Array XP à des fins telles que la duplication ou la sauvegarde de données, ou la récupération après sinistre. Les opérations en accès continu impliquent les baies de disques principales et distantes (secondaires). Les premières concernent les volumes principaux AC (P-VOL), contenant les données d'origine, qui sont connectés au système d'application. Les secondes contiennent les volumes secondaires AC (S-VOL) qui sont connectés au système de sauvegarde.
Voir aussi **BC** *(terme spécifique à HP StorageWorks Disk Array XP)*, **unité de commande principale** et **LDEV HP StorageWorks Disk Array XP**.

ACSLS *(terme spécifique à StorageTek*)
Automated Cartridge System Library Server, serveur de bibliothèque à système de cartouche automatisé - logiciel chargé de la gestion du système de cartouche automatisé (ACS).

Active Directory *(terme spécifique à Windows*)
Service d'annuaire d'un réseau Windows. Il contient des informations sur les ressources du réseau et les rend accessibles aux utilisateurs et aux applications. Les services d'annuaire permettent de nommer, de décrire, de localiser, de consulter et de gérer les ressources de manière cohérente, quel que soit le système physique sur lequel elles résident.

adresse IP
Adresse numérique d'un système servant à l'identifier de manière unique sur le réseau. L'adresse IP est constituée de quatre groupes de chiffres séparés par des points.

affichage de sauvegarde
Data Protector propose plusieurs affichages pour les spécifications de sauvegarde : par type - en fonction du type de données disponibles pour les sauvegardes ou les modèles. Affichage par défaut. Par groupe - en fonction du groupe auquel les spécifications/ modèles de sauvegarde appartiennent. Par nom - en fonction du nom des spécifications/modèles de sauvegarde. Par gestionnaire - si vous utilisez le MoM, vous pouvez également définir l'affichage de sauvegarde en fonction du Gestionnaire de cellule auquel appartiennent les spécifications/modèles de sauvegarde.

agent d'application
Composant requis sur un client pour sauvegarder ou restaurer les intégrations de bases de données en ligne.
Voir aussi **agent de disque**.

agent de disque
Composant devant être installé sur un client pour que ce dernier puisse être sauvegardé et restauré. L'Agent de disque contrôle la lecture et l'écriture de données sur un disque. Pendant une session de sauvegarde, l'Agent de disque lit les données stockées sur un disque et les envoie à l'Agent de support qui les déplace ensuite vers le périphérique. Pendant une session de restauration, l'Agent de disque reçoit des données de l'Agent de support et les écrit sur le disque.

agent de support
Processus contrôlant la lecture et l'écriture de données sur un périphérique qui lui-même lit ou écrit des données sur un support (généralement une bande). Pendant une session de sauvegarde, un Agent de support reçoit des données de l'Agent de disque et les envoie au périphérique qui les écrit ensuite sur le support. Pendant une session de restauration, un Agent de support localise les données stockées sur le support de sauvegarde et les envoie à l'Agent de disque. qui les écrit ensuite sur le disque. Un Agent de support gère également le contrôle robotique d'une bibliothèque.

agent EMC Symmetrix (SYMA)

(terme spécifique à EMC Symmetrix)
Voir **agent Symmetrix (SYMA)**

agent HP StorageWorks EVA (hérité)
Module logiciel Data Protector exécutant les tâches requises pour l'intégration de HP StorageWorks Enterprise Virtual Array et fonctionnant sur HP StorageWorks EVA avec le logiciel Command View (CV) EVA version v3.1 ou inférieure et le micrologiciel EVA VCS version v3.01x ou inférieure.
Voir aussi **Command View (CV) EVA** et **agent HP StorageWorks EVA SMI-S**.

agent HP StorageWorks EVA SMI-S
Module logiciel Data Protector exécutant toutes les tâches requises pour l'intégration de HP StorageWorks Enterprise Virtual Array et fonctionnant sur HP StorageWorks EVA avec le logiciel Command View (CV) EVA v3.2 et supérieure. Avec l'Agent EVA SMI-S, le contrôle de la matrice s'effectue via le fournisseur de HP StorageWorks SMI-S EVA, lequel dirige les communications entre les requêtes entrantes et CV EVA.
Voir aussi **Command View (CV) EVA**, **fournisseur de HP StorageWorks SMI-S EVA** et **agent HP StorageWorks EVA (hérité)**.

agent SSE *(terme spécifique à HP StorageWorks Disk Array XP)*
Module logiciel Data Protector exécutant toutes les tâches nécessaires à

une intégration de sauvegarde Split Mirror. Il communique avec le système de stockage HP StorageWorks Disk Array XP à l'aide de l'utilitaire du Gestionnaire RAID XP (pour les systèmes HP-UX et Windows) ou de la bibliothèque du Gestionnaire RAID (pour les systèmes Solaris).

agent Symmetrix (SYMA) *(terme spécifique à EMC Symmetrix)*
Module logiciel Data Protector qui prépare l'environnement EMC Symmetrix aux opérations de sauvegarde et de restauration.

agents de disque simultanés
Nombre d'Agents de disque autorisés à envoyer des données simultanément à un Agent de support.

AML *(terme spécifique à EMASS/GRAU)*
Automated Mixed-Media library, bibliothèque de supports mixtes automatisée.

analyse
Fonction permettant d'identifier les supports contenus dans un périphérique. Cette fonction synchronise la MMDB avec les supports se trouvant aux emplacements sélectionnés (les logements d'une bibliothèque, par exemple).

analyse
Fonction permettant d'identifier les supports contenus dans un périphérique. Cette fonction synchronise la MMDB avec les supports se trouvant aux emplacements sélectionnés (les logements d'une bibliothèque, par exemple). Elle est utile pour analyser et vérifier le support effectivement présent dans le périphérique lorsque quelqu'un a manipulé le support manuellement sans utiliser Data Protector pour l'éjecter ou l'insérer, par exemple.

API C Lotus *(terme spécifique à Lotus Domino Server)*
Interface destinée à l'échange de données de sauvegarde et de récupération entre Lotus Domino Server et une solution de sauvegarde comme Data Protector.

API de sauvegarde
Programme Oracle servant d'interface entre l'utilitaire de sauvegarde/restauration d'Oracle et la couche de gestion des supports de sauvegarde/restauration. L'interface définit un ensemble de routines afin de permettre la lecture et l'écriture des données sur les supports de sauvegarde, ainsi que la création, la recherche et la suppression des fichiers de sauvegarde.

API de serveur de sauvegarde Sybase

(terme spécifique à Sybase)
Interface standard développée pour l'échange de données de sauvegarde et de récupération entre un serveur Sybase SQL et une solution de sauvegarde telle que Data Protector.

application compatible cluster
Application prenant en charge l'API cluster (Application Programming Interface). Chaque application compatible cluster déclare ses propres ressources stratégiques (volumes de disques (sous Microsoft Cluster Server), groupes de volumes (sous MC/ServiceGuard), services d'application, noms et adresses IP ...).

archivage des journaux *(terme spécifique à Lotus Domino Server*)
Mode de connexion à la base de données Lotus Domino Server qui permet de n'écraser les fichiers de journal de transactions qu'après leur sauvegarde.

BACKINT *(terme spécifique à SAP R/3)*
Par le biais d'une interface ouverte, les programmes de sauvegarde SAP R/3 peuvent appeler l'interface backint Data Protector, laquelle leur permet de communiquer avec le logiciel Data Protector. En ce qui concerne la restauration et la sauvegarde, les programmes SAP R/3 émettent des ordres destinés à l'interface backint Data Protector.

banque de boîtes aux lettres (*terme spécifique à Microsoft Exchange Server 2000/2003)*
Partie de la banque d'informations conservant les informations relatives aux boîtes aux lettres des utilisateurs. Une banque de boîtes aux lettres est constituée d'un fichier binaire RTF .edb et d'un fichier de contenu Internet natif continu .stm.

banque de dossiers publics (*terme spécifique à Microsoft Exchange Server 2000/2003)*
Partie de la banque d'informations conservant les informations se trouvant dans les dossiers publics. Une banque de dossiers publics est constituée d'un fichier binaire RTF .edb et d'un fichier de contenu Internet natif continu .stm.

banque de répertoires (DS, pour Directory Store) *(terme spécifique à Microsoft Exchange)*
Partie du répertoire Microsoft Exchange Server. Ce répertoire contient des objets permettant aux applications Microsoft Exchange de rechercher et d'accéder aux services, boîtes aux lettres, destinataires, dossiers publics et autres objets pouvant être adressés au sein du

système de messagerie.
Voir aussi **banque d'informations (MDB)**.

banque d'informations *(terme spécifique à Microsoft Exchange Server 2000/2003)*
Service Microsoft Exchange Server 2000/2003 en charge de la gestion du stockage. La banque d'informations de Microsoft Exchange Server 2000/2003 gère deux types de banques : les boîtes aux lettres et les dossiers publics. Une banque de boîtes aux lettres appartenant à des utilisateurs individuels. Une banque d'informations publiques contient des dossiers et des messages publics partagés entre plusieurs utilisateurs.
Voir aussi **service Gestionnaire de clés** et **service de réplication de sites**.

banque d'informations *(terme spécifique à Microsoft Exchange Server 5.5)*
Fournisseur de banque de messages par défaut pour Microsoft Exchange Server 5.5. La banque d'informations est constituée des éléments suivants :

- Banque d'informations publique.
- Banque d'informations privée.
- Banque de dossiers personnels.
- Banque d'informations hors ligne.

La banque d'informations publiques contient des dossiers et des messages publics pouvant être partagés entre plusieurs utilisateurs et applications. Tous les utilisateurs partagent une seule banque d'informations publique au sein d'une organisation Microsoft Exchange Server 5.5, même lorsque le système utilise plusieurs serveurs Exchange. La banque d'informations privées est constituée de boîtes aux lettres pouvant appartenir à des utilisateurs ou à des applications. Les boîtes aux lettres résident sur le serveur sur lequel s'exécute Microsoft Exchange Server 5.5.
Voir aussi **banque de répertoires (DS)**.

banque d'informations privées *(terme spécifique à Microsoft Exchange Server 5.5)*
Partie de la banque d'informations conservant les informations se trouvant dans les boîtes aux lettres des utilisateurs. Une banque de boîtes aux lettres est constituée d'un fichier binaire RTF .edb.

basculement
Transfert des données de cluster les plus importantes, également appelées groupe (Windows) ou package (Unix), d'un nœud de cluster à un autre. Un basculement peut se produire en raison de défaillances logicielles ou

matérielles, ou d'opérations de maintenance au niveau du nœud primaire.

base de données centralisée de gestion des supports (CMMDB)
Voir **CMMDB**.

base de données cible *(terme spécifique à Oracle)*
Terme utilisé dans le contexte du Gestionnaire de récupération (RMAN). La base de données cible est celle qui est sauvegardée ou restaurée.

base de données de registres COM+ *(terme spécifique à Windows)*
La base de données de registres COM+ et la base de registres Windows stockent les attributs d'applications, de classes et de matériels COM+. Elles garantissent ainsi la cohérence entre ces attributs et assurent un fonctionnement courant pour gérer ces derniers.

base de données du catalogue de récupération *(terme spécifique à Oracle)*
Base de données Oracle contenant un schéma de catalogue de récupération. Ne stockez pas le catalogue de récupération dans votre base de données cible.

base de données du gestionnaire de supports amovibles *(terme spécifique à Windows)*
Service Windows pour la gestion de supports amovibles (tels que des bandes et des disques) et de périphériques de stockage (bibliothèques). Le stockage sur périphériques amovibles permet aux applications d'accéder aux mêmes ressources et de les partager.

bases de données système *(terme spécifique à Sybase)*
Les quatre bases de données système d'un Sybase SQL Server nouvellement installé sont les suivantes :

- Base de données principale (master).
- Base de données temporaire (tempdb).
- Base de données de procédure système (sybsystemprocs).
- Base de données modèle (model).

base de données ZDB *(terme spécifique à ZBD)*
Partie de la base de données IDB stockant des informations relatives à ZDB telles que les volumes source, les répliques et des informations relatives à la sécurité. La base de données ZDB est utilisée pour ZDB (sauvegarde avec temps d'indisponibilité nul), pour les restaurations instantanées et Split

Mirror.
Voir aussi **sauvegarde avec temps d'indisponibilité nul (ZDB)**.

BC *(terme spécifique à EMC Symmetrix)*
Business Continuance - Procédé permettant aux utilisateurs d'accéder et de gérer des copies instantanées des périphériques standard EMC Symmetrix.
Voir aussi **BCV**.

BC *(terme spécifique à HP StorageWorks Disk Array XP)*
La Business Copy XP permet à l'utilisateur de conserver des copies internes des LDEV HP StorageWorks Disk Array XP, notamment à des fins de sauvegarde ou de duplication de données. Les copies (volumes secondaires ou S-VOL) peuvent être séparées des volumes principaux (P-VOL) et connectées à un système différent, à des fins aussi diverses que la sauvegarde ou le développement. En ce qui concerne la sauvegarde, les P-VOL doivent être connectés au système d'application ; l'un des jeux de miroirs S-VOL doit, quant à lui, être connecté au système de sauvegarde.
Voir aussi **HP StorageWorks Disk Array XP LDEV**, **CA**, **unité de commande principale**, **système d'application** et **système de sauvegarde**.

BCV *(terme spécifique à EMC Symmetrix)*
Business Continuance Volumes ou périphériques BCV - il s'agit de SLD dédiés, préconfigurés dans l'ICDA sur lequel l'opération Business Continuance est exécutée. Des adresses SCSI distinctes, lesquelles diffèrent des adresses utilisées par les SLD dont elles sont le miroir, sont attribuées aux périphériques BCV. Ces derniers sont utilisés comme miroirs séparables des SLD EMC Symmetrix principaux devant être protégés.
Voir aussi **BC** et **Processus BC**.

BC VA *(terme spécifique HP StorageWorks Virtual Array)*
Business Copy VA vous permet de conserver des copies internes des LUN HP StorageWorks Virtual Array pour la sauvegarde ou la duplication de données dans une même baie de virtualisation. Les copies (LUN enfants ou Business Copy) peuvent être utilisées à des fins aussi diverses que la sauvegarde, l'analyse de données ou le développement. Lorsqu'ils sont utilisés à des fins de sauvegarde, les LUN d'origine (parents) sont connectés au système d'applications. Les LUN Business Copy (enfants) sont, quant à eux, connectés au système de sauvegarde.
Voir aussi **LUN HP StorageWorks Virtual Array**, **système d'application** et **système de sauvegarde**.

bibliothèque
Egalement appelée “changeur automatique”, “bibliothèque de banques magnéto-optiques”, “chargeur automatique” ou “échangeur”. Une bibliothèque contient des supports stockés dans des emplacements référentiels. Chaque emplacement contient un support (par exemple, DDS/DAT). Les supports sont déplacés entre les emplacements et les lecteurs par un mécanisme robotique permettant un accès aléatoire aux supports. Une bibliothèque peut contenir plusieurs lecteurs.

bibliothèque ACS StorageTek
(terme spécifique à StorageTek)
Système de bibliothèque (également connu sous le nom de “silo”) constitué d’une unité de gestion de bibliothèque (LMU) et d’un à vingt-quatre modules de stockage en bibliothèque (LSM) connectés à l’unité.

bibliothèque de bandes magnéto-optiques
Voir **bibliothèque**.

bibliothèque de base de données
Ensemble de routines Data Protector permettant le transfert de données entre Data Protector et le serveur d’une intégration de base de données en ligne, le serveur Oracle par exemple.

bibliothèque du Gestionnaire RAID

(terme spécifique à HP StorageWorks Disk Array XP)
Bibliothèque utilisée en interne par Data Protector sur les systèmes Solaris pour permettre l’accès aux données de configuration, d’état et de performances de HP StorageWorks Disk Array XP, ainsi qu’aux fonctions clé de HP StorageWorks Disk Array XP, au moyen d’appels de fonction convertis en une séquence de commandes SCSI de bas niveau.

boîte aux lettres (*(terme spécifique à Microsoft Exchange Server)*
Emplacement où sont livrés les messages électroniques. Cet emplacement est défini par l’administrateur pour chaque utilisateur. Si un ensemble de dossiers personnels est désigné comme emplacement de distribution du courrier électronique, les messages sont acheminés de la boîte aux lettres vers cet emplacement.

BRARCHIVE *(terme spécifique à SAP R/3)*
Outil de sauvegarde SAP R/3 permettant à l’utilisateur d’archiver les fichiers journaux de rétablissement. BRARCHIVE permet également d’enregistrer l’ensemble des journaux et profils du processus d’archivage.
Voir aussi **SAPDBA**, **BRBACKUP** et **BRRESTORE**.

BRBACKUP *(terme spécifique à SAP R/3)*
Outil de sauvegarde SAP R/3 permettant d'effectuer une sauvegarde en ligne ou hors ligne du fichier de contrôle, de fichiers de données distincts ou de l'ensemble des espaces de tables et, le cas échéant, des fichiers journaux de rétablissement en ligne.
Voir aussi **SAPDBA**, **BRARCHIVE** et **BRRESTORE**.

BRRESTORE *(terme spécifique à SAP R/3)*
Outil de sauvegarde SAP R/3 permettant de restaurer les types de fichier suivants :

- Fichiers de données de base de données, fichiers de contrôle et fichiers journaux de rétablissement en ligne sauvegardés avec BRBACKUP.
- Fichiers journaux de rétablissement archivés avec BRARCHIVE.
- Fichiers non base de données sauvegardés avec BRBACKUP.

Vous pouvez spécifier des fichiers, des espaces de table, des sauvegardes complètes, des numéros de séquence de fichiers journaux de rétablissement ou l'ID de session de la sauvegarde.
Voir aussi **SAPDBA**, **BRBACKUP** et **BRARCHIVE**.

BSM
Le Backup Session Manager Data Protector (Gestionnaire de session de sauvegarde) contrôle la session de sauvegarde. Ce processus est toujours exécuté sur le système du Gestionnaire de cellule.

canal *(terme spécifique à Oracle*)
Allocation de ressources du Gestionnaire de récupération Oracle. Chaque canal alloué lance un nouveau processus Oracle qui effectue des actions de sauvegarde, de restauration et de récupération. Le type de canal affecté détermine le type de support utilisé :

- Type "disque".
- Type "SBT_TAPE".

Si le canal spécifié est de type "SBT_TAPE" et qu'Oracle est intégré à Data Protector, le processus du serveur essaie de lire les sauvegardes ou d'écrire les fichiers de données sur Data Protector.

CAP *(terme spécifique à StorageTek*)
Cartridge Access Port - port d'accès intégré au panneau porte d'une bibliothèque permettant d'insérer ou d'éjecter les supports.

caractère générique
Caractère pouvant être utilisé pour représenter un ou plusieurs caractères.

Par exemple, l'astérisque (*) représente généralement un ou plusieurs caractères et le point d'interrogation (?) un seul caractère. Les caractères génériques sont souvent utilisés avec les systèmes d'exploitation pour spécifier plusieurs fichiers par nom.

catalogue de récupération *(terme spécifique à Oracle)*
Ensemble de tables et de vues Oracle permettant au Gestionnaire de récupération de stocker des informations sur les bases de données Oracle. Grâce à ces informations, le Gestionnaire de récupération peut gérer la sauvegarde, la restauration et la récupération des bases de données Oracle. Le catalogue de récupération contient des informations sur :

- Le schéma physique de la base de données cible Oracle.
- Les jeux de sauvegarde de fichiers de données et de journaux d'archive.
- Les copies de fichiers de données.
- Les journaux de rétablissement archivés.
- Les scripts stockés.

CDB
Catalog Database, Base de données du catalogue - Il s'agit d'une partie de la base de données IDB contenant des informations sur les sauvegardes, les copies d'objet, les restaurations, les sessions de gestion de supports ainsi que sur les données sauvegardées. En fonction du niveau de journalisation sélectionné, la CDB contient également les noms et versions de fichiers. Cette partie de la base de données se trouve toujours dans la cellule locale.
Voir aussi **MMDB**.

cellule
Ensemble de systèmes contrôlés par un gestionnaire de cellule. Une cellule représente habituellement les systèmes d'un site ou d'une entité organisationnelle qui sont connectés à un même réseau local. Un contrôle centralisé permet d'administrer les tâches et les stratégies de sauvegarde et de restauration.

chaîne de périphériques
Série de périphériques autonomes configurés pour une utilisation séquentielle. Lorsqu'un support est plein dans un périphérique, la sauvegarde se poursuit automatiquement sur un support du périphérique suivant dans la chaîne de périphériques.

chaîne de sauvegarde
Désigne une situation dans laquelle des sauvegardes complètes et incrémentales sont effectuées. En fonction du niveau de sauvegarde incrémentale utilisé (Incr,

Incr 1, Incr 2, etc.), des dépendances simples ou relativement complexes relient les sauvegardes incrémentales en cours aux sauvegardes incrémentales antérieures. La chaîne de sauvegarde désigne l'ensemble des sauvegardes, débutant par les sauvegardes complètes et complété par toutes les sauvegardes incrémentales jusqu'au point voulu dans le temps.

changeur automatique
Voir aussi **bibliothèque**.

chargeur automatique
Voir aussi **bibliothèque**.

chargeurs
Périphériques possédant plusieurs emplacements destinés au stockage des supports et disposant généralement d'un seul lecteur. Un chargeur sélectionne les supports dans une pile de manière séquentielle. Une bibliothèque, en revanche, peut sélectionner les supports de manière aléatoire depuis son référentiel.

clé de session
Cette variable d'environnement pour les scripts de pré-exécution et de post-exécution constitue une identification unique de session dans Data Protector, y compris pour les sessions de test. Elle n'est pas enregistrée dans la base de données, et sert à spécifier les commandes d'interface de ligne de commande omnimnt, omnistat et omniabort.

client dynamique
Voir **sauvegarde de client avec découverte de disque**.

client ou **système client**
Tout système configuré avec des fonctions Data Protector et dans une cellule.

CMMDB
Centralized Media Management Database, base de données centralisée de gestion des supports - La CMMDB Data Protector résulte de la fusion des bases de données de gestion des supports à partir de plusieurs cellules dans l'environnement MoM. Elle permet à l'utilisateur de partager des supports et périphériques haut de gamme avec plusieurs cellules dans un environnement MoM. Une cellule peut contrôler les systèmes robotiques desservant les périphériques connectés à des systèmes se trouvant dans d'autres cellules.
La CMMDB doit résider sur le Gestionnaire MoM. Une connexion réseau fiable entre la cellule MoM et les autres cellules Data Protector est fortement recommandée.
Voir aussi **MoM**.

Command View (CV) EVA *(terme spécifique à HP StorageWorks)*
Interface utilisateur permettant de configurer, d'administrer et de surveiller votre système de stockage HP StorageWorks EVA. Cet interface est utilisée pour effectuer diverses tâches de gestion du stockage, par exemple, la création de familles de disques virtuels, la gestion du matériel de stockage, la création de snapclones et de snapshots de disques virtuels. Le logiciel Command View EVA s'exécute sur l'appareil de gestion du stockage HP OpenView. Il est accessible via un navigateur Web.
Voir aussi **agent HP StorageWorks EVA (hérité)** et **agent HP StorageWorks EVA SMI-S**.

commandes pré- et post-exécution
Les commandes pré- et post-exécution servent à réaliser une action supplémentaire avant et après une session de sauvegarde ou de restauration. Elles ne sont pas fournies avec Data Protector. L'utilisateur doit les créer lui-même. Elles peuvent être rédigées sous la forme de programmes exécutables ou de fichiers séquentiels sous Windows, ou bien de scripts shell sous UNIX.

compte utilisateur
Vous ne pouvez utiliser Data Protector que si vous disposez d'un compte utilisateur Data Protector, lequel limite l'accès non autorisé à Data Protector et aux données sauvegardées. Les administrateurs Data Protector créent ce compte en spécifiant un nom d'utilisateur, les systèmes à partir desquels l'utilisateur peut se connecter et le groupe d'utilisateurs Data Protector auquel il sera affecté. Ces spécifications sont vérifiées chaque fois que l'utilisateur démarre l'interface Data Protector ou effectue certaines tâches.

compte utilisateur Data Protector
Vous ne pouvez utiliser Data Protector que si vous disposez d'un compte utilisateur Data Protector, lequel limite l'accès non autorisé à Data Protector et aux données sauvegardées. Les administrateurs Data Protector créent ce compte en spécifiant un nom d'utilisateur, les systèmes à partir desquels l'utilisateur peut se connecter et le groupe d'utilisateurs Data Protector auquel il sera affecté. Ces spécifications sont vérifiées chaque fois que l'utilisateur démarre l'interface Data Protector ou effectue certaines tâches.

contrôleur de domaine
Un serveur d'un réseau responsable de la sécurité de l'utilisateur et de la vérification des mots de passe dans un groupe d'autres serveurs.

copie d'objet
Copie d'une version d'un objet spécifique créé au cours d'une session

de copie d'objet ou une session de sauvegarde avec mise en miroir des objets.

copie miroir *(terme spécifique à MS VSS)*
Volume représentant une copie du volume d'origine à un instant donné. La sauvegarde de données s'effectue alors depuis la copie miroir, et non depuis le volume d'origine. Le volume d'origine change à mesure que le processus de sauvegarde se poursuit ; la copie miroir, en revanche, demeure identique.
Voir aussi **service Microsoft Volume Shadow Copy**.

création de snapshot *(terme spécifique à HP StorageWorks VA et HP StorageWorks EVA)*
Technique de création de répliques dans laquelle les copies des volumes source sont créées via l'utilisation de techniques de virtualisation du stockage. Les copies sont considérées comme créées à un instant donné bien précis, sans pré-configuration et immédiatement disponibles pour utilisation. Cependant, les processus de copie en arrière-plan se poursuivent après la création.
Voir aussi **snapshot**.

création de split mirror *(terme spécifique à EMC Symmetrix et HP StorageWorks Disk Array XP)*
Technique de création de répliques selon laquelle un ensemble de volumes cible pré-configuré (un miroir) est synchronisé avec un ensemble de volumes source jusqu'à ce qu'une réplique du contenu des volumes source soit requise. La synchronisation est ensuite interrompue (le miroir est divisé) et une réplique split mirror des volumes source au moment de la division reste dans les volumes cible.
Voir aussi **split mirror**.

CRS
Le processus CRS (Cell Request Server) s'exécute sur le Gestionnaire de cellule Data Protector. Il lance et contrôle les sessions de sauvegarde et de restauration. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.
Le CRS s'exécute sous le compte root sur les systèmes UNIX et sous tout compte Windows. Par défaut, il s'exécute sous le compte de l'utilisateur spécifié lors de l'installation.

CSM
Le processus Copy Session Manager Data Protector (Gestionnaire de session de copie) contrôle la session de copie d'objet et s'exécute sur le système Gestionnaire de cellule.

Dbobject *(terme spécifique à Informix)*
Objet base de données physique Informix. Il peut s'agir d'un blobspace, d'un dbspace ou d'un fichier journal logique.

DCBF
Les fichiers binaires de catalogue des détails (DCBF) font partie de la base de données IDB. Ils contiennent les informations relatives aux attributs et aux versions de fichier et occupent environ 80 % de la base de données IDB. Par défaut, ces fichiers sont contenus dans un répertoire DC dont la taille maximale est de 2 Go. Vous pouvez créer d'autres répertoires DC.

découverte des disques
Détection des disques au cours de la sauvegarde d'un client avec découverte des disques. Lors de cette sauvegarde, Data Protector découvre (détecte) les disques présents sur le client (même s'ils ne l'étaient pas lors de la configuration de la sauvegarde) et les sauvegarde. Ce type de sauvegarde est très utile dans les environnements dynamiques où les configurations changent rapidement. Une fois les disques développés, chacun d'entre eux hérite de toutes les options de son objet client principal. Même si les commandes pré- et post-exécution ne sont spécifiées qu'une seule fois, elles sont démarrées à plusieurs reprises, à raison d'une fois par objet.

demande de montage
Message apparaissant à l'écran et invitant l'utilisateur à insérer un support spécifique dans un périphérique. Lorsque vous avez répondu à la demande de montage en fournissant le support requis et en confirmant, la session se poursuit.

dépôt de fichiers
Fichier contenant les données d'une sauvegarde sur un périphérique de bibliothèque de fichiers.

disque système
Disque contenant les fichiers du système d'exploitation. La terminologie utilisée par Microsoft définit le disque système comme un disque contenant les fichiers nécessaires pour assurer les premières étapes du processus d'amorçage.

disque virtuel *(terme spécifique à HP StorageWorks)*
Unité de stockage attribuée à partir d'un pool de disques HP StorageWorks Enterprise Virtual Array. Les disques virtuels sont les entités dupliquées à l'aide de la fonctionnalité de sauvegarde de HP StorageWorks Enterprise Virtual Array.
Voir aussi **volume source** et **volume cible**.

disques partagés
Disque Windows situé sur un autre système qui a été mis à la disposition

d'autres utilisateurs du réseau. Les sytèmes dotés de disques partagés peuvent être sauvegardés, même en l'absence d'un Agent de disque Data Protector.

DMZ
La zone démilitarisée (DMZ) est un réseau inséré en tant que "zone neutre" entre le réseau privé d'une société (intranet) et le réseau public extérieur (Internet). Elle empêche les utilisateurs externes d'accéder directement aux serveurs de la société sur l'intranet de celle-ci.

données sauvegardées publiques/ privées
Lors de la configuration d'une sauvegarde, l'utilisateur peut indiquer si les données sauvegardées seront :

- Publiques, c'est-à-dire visibles (et accessibles pour la restauration) à tous les utilisateurs Data Protector.
- Privées, c'est-à-dire visibles (et accessibles pour la restauration) uniquement au propriétaire de la sauvegarde et aux administrateurs.

DR OS
Un système d'exploitation pour récupération après sinistre est un système d'exploitation dans lequel la récupération après sinistre s'effectue. Il fournit à Data Protector un environnement d'exécution de base (accès au disque, réseau, bande et au système de fichiers). Le système d'exploitation doit être installé et configuré pour que la récupération après sinistre Data Protector puisse être effectuée. Le DR OS héberge non seulement le processus de récupération après sinistre Data Protector, mais fait également partie du système restauré car il remplace ses propres données de configuration par les données de configuration d'origine.

droits d'accès
Voir **droits utilisateurs**.

droits utilisateur
Les droits utilisateur ou droits d'accès correspondent aux autorisations nécessaires pour exécuter certaines tâches dans Data Protector, telles que la configuration d'une sauvegarde, le démarrage d'une session de sauvegarde ou le lancement d'une session de restauration. Les utilisateurs disposent des droits d'accès du groupe d'utilisateurs auquel ils appartiennent.

échangeur
Egalement appelé échangeur SCSI. *Voir aussi* **bibliothèque**.

emplacement
Position mécanique au sein d'une bibliothèque. Chaque emplacement peut contenir un support, comme une bande

DLT. Data Protector attribue un numéro à chaque emplacement. Pour être lu, un support est déplacé par un mécanisme robotique de son emplacement dans le lecteur.

emplacement d'un support
Emplacement physique d'un support défini par l'utilisateur, tel que "bâtiment 4" ou "stockage hors site".

enregistrement circulaire *(terme spécifique à Microsoft Exchange Server et Lotus Domino Server*)
L'enregistrement circulaire est un mode de base de données Microsoft Exchange Server et Lotus Domino Server, dans lequel le contenu du fichier du journal de transactions est périodiquement écrasé une fois les données correspondantes validées dans la base de données. L'enregistrement circulaire réduit les besoins en espace disque.

environnement de sauvegarde d'entreprise
Plusieurs cellules peuvent être regroupées et gérées depuis une cellule centrale. L'environnement de sauvegarde d'entreprise comprend tous les clients répartis entre plusieurs cellules Data Protector, lesquelles sont gérées et administrées à partir d'une cellule centrale utilisant le concept Manager-of-Managers.
Voir aussi **MoM**.

espace de table
Partie de la structure d'une base de données. Chaque base de données est divisée de manière logique en un ou plusieurs espaces de table. Chaque espace de table contient des fichiers de données ou des volumes bruts qui lui sont exclusivement associés.

établissement (rétablissement) incrémentiel *(terme spécifique à EMC Symmetrix)*
Opération de contrôle BCV ou SRDF. Dans les opérations de contrôle BCV, un établissement incrémentiel entraîne la synchronisation incrémentale du périphérique BCV et son fonctionnement en tant que support EMC Symmetrix miroir. Des paires doivent avoir été préalablement définies entre les périphériques EMC Symmetrix.
Dans les opérations de contrôle SRDF, un établissement incrémental entraîne la synchronisation incrémentale du périphérique (R2) cible et son fonctionnement en tant que support EMC Symmetrix miroir. Des paires doivent avoir été préalablement définies entre les périphériques EMC Symmetrix.

état de paire *(terme spécifique à HP StorageWorks Disk Array XP*)
Une paire de disques miroir peut avoir

différentes valeurs d'état, selon l'action effectuée. Les trois valeurs d'état les plus importantes sont les suivantes :

- COPY - La paire mise en miroir est en cours de resynchronisation. Les données sont transférées d'un disque à l'autre. Les disques ne contiennent pas les mêmes données.

- PAIR - La paire mise en miroir est complètement synchronisée et les données stockées sur les deux disques (le volume principal et le volume miroir) sont identiques.

- SUSPENDED - Le lien entre les disques miroir est suspendu. Cela signifie qu'il est possible d'accéder aux disques et de les mettre à jour indépendamment. Toutefois, la relation de miroir est maintenue et la paire de disques peut être resynchronisée sans pour autant effectuer un transfert complet du contenu du disque.

état des supports
Qualité des supports telle qu'elle est reflétée par les facteurs d'état des supports. Plus l'âge et l'utilisation faite des supports sont importants, plus les risques d'erreurs de lecture et d'écriture sont élevés sur les supports à bande. Un support doit être remplacé lorsque son état est MEDIOCRE.

état système *(terme spécifique à Windows)*
Les données d'état système comprennent le registre, la base de données d'enregistrement de classe COM+, les fichiers de démarrage système et la base de données de services de certificats (à condition que le serveur soit du type "certificate server"). Si le serveur est un contrôleur de domaine, les données d'état système contiennent également le service d'annuaire Active Directory et le répertoire Sysvol. Si le serveur exécute le service de cluster, les données d'état système comprennent également les points de contrôle du registre de ressource et le journal de récupération de ressource quorum, qui contient les informations les plus récentes concernant la base de données de clusters.

étiquette de support
Identificateur défini par l'utilisateur et servant à décrire un support.

exportation de supports
Procédé consistant à supprimer de la base de données IDB toutes les données relatives aux sessions de sauvegarde (comme les systèmes, objets et noms des fichiers qui résident sur le support). Les informations relatives aux supports et à leur relation par rapport à un pool sont également supprimées de la base de données IDB. Toutefois, les données

enregistrées sur les supports restent inchangées.
Voir aussi **importation de supports.**

facteurs d'état des supports
Limites d'âge et de réécriture définies par l'utilisateur pour déterminer l'état d'un support.

Fibre Channel
Norme ANSI pour l'interconnexion informatique à haute vitesse. Utilisant des câbles à fibre optique ou en cuivre, cette technologie permet la transmission bidirectionnelle ultra-rapide de fichiers de données volumineux, et peut être déployée entre des sites distants de plusieurs kilomètres.
La technologie Fibre Channel relie les nœuds au moyen de trois topologies physiques différentes : point à point, en boucle et par commutation.

fichier CDF *(terme spécifique à UNIX)*
Context Dependent File, fichier contextuel - Il s'agit d'un fichier constitué de plusieurs fichiers regroupés sous le même chemin d'accès. Le système sélectionne habituellement l'un des fichiers à l'aide du contexte du processus. Ce mécanisme permet à des exécutables dépendant des machines, à des fichiers de données système et à des fichiers de périphériques de fonctionner correctement depuis l'ensemble des hôtes d'un cluster, tout en utilisant le même chemin d'accès.

fichier d'amorçage d'urgence *(terme spécifique à Informix)*
Fichier de configuration Informix résidant dans le répertoire *<INFORMIXDIR>*\etc (sur HP-UX) ou *<INFORMIXDIR>*/etc (sous Windows) et appelé ixbar.*<id_serveur>*, où *<INFORMIXDIR>* correspond au répertoire de base du serveur en ligne et *<id_serveur>* à la valeur du paramètre de configuration SERVERNUM. Chaque ligne du fichier d'amorçage d'urgence correspond à un objet sauvegarde.

fichier de base de données de ligne de commande EMC Symmetrix *(terme spécifique à EMC Symmetrix)*
Voir **fichier de base de données de ligne de commande Symmetrix**

fichier de base de données de ligne de commande Symmetrix
(terme spécifique à EMC Symmetrix)
Fichier de base de données EMC Symmetrix stockant les données de configuration EMC Symmetrix sur chaque système disposant d'une baie de disques intégrée (ICDA) et d'une interface de ligne de commande (SYMCLI) EMC Symmetrix.

fichier de contrôle *(terme spécifique à Oracle et SAP R/3)*
Fichier de données Oracle contenant des entrées spécifiant la structure physique de la base de données. Il fournit des

informations sur la cohérence de la base de données utilisées pour la récupération.

fichier de données *(terme spécifique à Oracle et SAP R/3*)
Fichier physique créé par Oracle et contenant des structures de données telles que les tables et index. Un fichier de données ne peut appartenir qu'à une seule base de données Oracle.

fichier d'options globales
Fichier permettant à l'utilisateur de personnaliser Data Protector. Ce fichier fournit des informations sur les options globales, lesquelles concernent différents aspects de Data Protector, généralement les délais d'attente et les limites, et affectent la cellule Data Protector entière. Le fichier est situé dans le répertoire /etc/opt/omni/server/options sur les systèmes HP-UX et Solaris et dans le répertoire <*répertoire_Data_Protector*>\Config\Server\Options sur les systèmes Windows.

fichier DRS
Le fichier de données de récupération système (DRS) Data Protector contient les informations système requises pour l'installation et la configuration du système d'exploitation en cas de sinistre. Il s'agit d'un fichier ASCII généré lorsque la sauvegarde de la CONFIGURATION est effectuée sur un client Windows, puis stockée sur le Gestionnaire de cellule.

fichier épars Fichier contenant des données avec des parties de bloc vides. Exemples : matrice dont une partie ou la plupart des données contient des zéros ; fichiers provenant d'applications de visualisation d'images ; bases de données rapides. Si l'option de traitement des fichiers épars n'est pas activée pendant la restauration, il se peut que la restauration soit impossible.

fichier jours chômés
Fichier contenant des informations sur les jours chômés. Vous pouvez définir des jours chômés différents en modifiant le fichier Jours chômés : /etc/opt/omni/server/Holidays sur le Gestionnaire de cellule UNIX et <*répertoire_Data_Protector*>\Config\Server\holidays sur le Gestionnaire de cellule Windows.

fichier P1S
Fichier P1S contenant des informations sur le formatage et le partitionnement de tous les disques installés sur un système lors d'une récupération après sinistre automatisée évoluée (EADR). Il est créé lors d'une sauvegarde complète et enregistré sur un support de sauvegarde et sur le Gestionnaire de cellule dans le répertoire <*répertoire_Data_Protector*>\Config\Server\dr\p1s sur un

Gestionnaire de cellule Windows, ou dans le répertoire /etc/opt/omni/server/dr/p1s sur un Gestionnaire de cellule UNIX, sous le nom recovery.p1s.

fichier sqlhosts *(terme spécifique à Informix*)
Fichier d'informations de connectivité Informix contenant les noms de tous les serveurs de base de données, ainsi que tous les alias auxquels les clients d'un ordinateur hôte peuvent se connecter.

fichier sst.conf
Le fichier /usr/kernel/drv/sst.conf doit être présent sur chaque client Sun Solaris Data Protector auquel un périphérique de bibliothèque multi-lecteurs est connecté. Il doit contenir une entrée pour l'adresse SCSI du mécanisme robotique de chaque périphérique de bibliothèque connecté au client.

fichier st.conf
Le fichier /kernel/drv/st.conf doit être présent sur chaque client Solaris Data Protector auquel un périphérique de sauvegarde est connecté. Il doit contenir des informations sur le périphérique et une adresse SCSI pour chaque lecteur de sauvegarde connecté au client. Une seule entrée SCSI est requise pour un périphérique à lecteur unique, tandis qu'il en faut plusieurs pour un périphérique de bibliothèque multi-lecteurs.

fichier TSANDS.CFG *(terme spécifique à Novell NetWare)*
Fichier permettant à l'utilisateur de spécifier les noms des conteneurs à partir desquels les sauvegardes doivent commencer. Il s'agit d'un fichier texte situé dans le répertoire SYS:SYSTEM\TSA du serveur où est chargé TSANDS.NLM.

fichiers de journal des transactions
Fichiers enregistrant les transactions relatives aux modifications de la base de données, et assurent la tolérance de panne en cas de sinistre de la base de données.

fichiers journaux logiques
Concerne la sauvegarde de base de données en ligne. Les fichiers journaux logiques sont des fichiers dans lesquels les données modifiées sont stockées avant d'être transférées au disque. En cas de panne, les fichiers journaux logiques permettent de repositionner toutes les transactions qui ont été transférées et d'annuler toutes celles qui ne l'ont pas encore été.

flux de données
Séquence de données transférées via le canal de communication.

fnames.dat
Les fichiers fnames.dat de la base de données IDB contiennent des informations sur les noms des fichiers

sauvegardés. Ces fichiers occupent généralement 20 % environ de la base de données IDB si des noms de fichiers sont stockés.

formatage
Processus consistant à effacer toutes les données contenues sur un support et à préparer ce dernier pour l'utiliser avec Data Protector. Les informations relatives au support (ID du support, description et emplacement) sont enregistrées dans la base IDB ainsi que sur les supports concernés (en en-tête de ces derniers). Les supports Data Protector comportant des données protégées ne sont pas formatés tant que la protection n'a pas expiré ou que la protection du support n'est pas retirée ou le support recyclé.

fournisseur de copie miroir *(terme spécifique à MS VSS)*
Entité réalisant la création et la représentation des copies miroir des volumes. Les fournisseurs possèdent les données des copies miroir et exposent les copies miroir. Ils peuvent être de type logiciel (par exemple, les fournisseurs système) ou matériel (disques locaux, baies de disques).
Voir aussi **copie miroir.**

Fournisseur de HP StorageWorks SMI-S EVA
Interface permettant de contrôler HP StorageWorks Enterprise Virtual Array. Le fournisseur de SMI-S EVA est utilisé comme service distinct sur l'appareil de gestion du stockage HP OpenView et agit comme passerelle entre les requêtes entrantes et Command View EVA. Avec l'intégration de Data Protector HP StorageWorks EVA, le fournisseur de SMI-S EVA accepte les requêtes standardisées de l'Agent EVA SMI-S, communique avec Command View EVA pour l'appel d'informations ou de méthodes et renvoie des réponses standardisées.
Voir aussi **agent HP StorageWorks EVA SMI-S** et **Command View (CV) EVA**.

fusion
La fusion correspond à un mode de résolution de conflit de fichiers au cours d'une restauration. Si le fichier à restaurer se trouve déjà à l'emplacement de destination, c'est celui dont la date de modification est la plus récente qui est conservé. Les fichiers qui ne sont pas présents sur le disque sont toujours restaurés.
Voir aussi **réécriture**.

génération de sauvegarde
Une génération de sauvegarde est constituée d'une sauvegarde complète et de toutes les sauvegardes incrémentales effectuées jusqu'à la sauvegarde complète suivante.

Gestion de stockage hiérarchique (HSM, pour Hierarchical Storage Management)
Méthode visant à optimiser l'utilisation de l'espace disque pour le stockage des données et consistant à faire migrer les données les moins souvent utilisées vers des disques optiques moins coûteux. Lorsque cela est nécessaire, les données migrent de nouveau sur le disque dur. Cette méthode permet de trouver un équilibre entre le besoin d'extraire rapidement les données du disque dur et l'utilisation de disques optiques moins coûteux.

Gestionnaire de cellule
Système principal de la cellule dans lequel est installé le logiciel Data Protector central et d'où sont gérées toutes les activités de sauvegarde et de restauration. L'interface graphique utilisée pour les opérations de gestion peut se trouver sur un système différent. Chaque cellule dispose d'un système de Gestionnaire de cellule.

Gestionnaire de clés *(terme spécifique à Microsoft Exchange Server 2000/ 2003)*
Service Microsoft Exchange Server 2000/2003 fournissant la fonction de cryptage pour une sécurité accrue. *Voir aussi* **banque d'informations** et **service de réplication de sites**.

gestionnaire de récupération (RMAN) *(terme spécifique à Oracle)*
Interface de ligne de commande Oracle contrôlant un processus du serveur Oracle pour la sauvegarde, la restauration ou la récupération de la base de données à laquelle il est connecté. RMAN stocke les informations sur les sauvegardes dans le catalogue de récupération ou dans le fichier de contrôle. Ces informations peuvent être utilisées lors de sessions de restauration ultérieures.

Gestionnaire RAID XP *(terme spécifique à HP StorageWorks Disk Array XP)*
L'application du Gestionnaire RAID XP met à disposition de l'utilisateur une liste complète de commandes permettant d'établir des rapports et de contrôler l'état des applications CA et BC. Ces commandes communiquent avec l'unité de commande de disque HP StorageWorks Disk Array XP par le biais d'une instance du Gestionnaire RAID. Cette instance convertit les commandes en une séquence de commandes SCSI de bas niveau.

groupe *(terme spécifique à Microsoft Cluster Server*)
Ensemble de ressources (par exemple, des volumes de disque, des services d'applications, des noms et adresses IP) nécessaires à l'exécution d'applications compatibles cluster spécifiques.

groupe de disques *(terme spécifique à Veritas Volume Manager)*
Unité de base de stockage des données dans un système VxVM. Un groupe de disques peut être constitué d'un ou plusieurs volumes physiques. Le système peut contenir plusieurs groupes de disques.

groupe de périphériques *(terme spécifique à EMC Symmetric*)
Unité logique représentant plusieurs périphériques EMC Symmetrix. Un même périphérique ne peut appartenir à plus d'un groupe de périphériques. Tous les périphériques d'un groupe doivent se trouver sur la même unité EMC Symmetrix. Les groupes de périphériques vous permettent d'identifier et d'utiliser un sous-ensemble de périphériques EMC Symmetrix disponibles.

groupe de stockage
(terme spécifique à Microsoft Exchange Server 2000/2003)
Ensemble de bases de données (banques) se partageant un jeu de fichiers de journal des transactions. Exchange gère chaque groupe de stockage au moyen d'un processus de serveur distinct.

groupe de volumes
Unité de stockage des données dans un système LVM. Un groupe de volumes peut être constitué d'un ou plusieurs volumes physiques. Le système peut contenir plusieurs groupes de volumes.

groupe d'utilisateurs
Chaque utilisateur de Data Protector est membre d'un groupe d'utilisateurs, et chaque utilisateur faisant partie d'un groupe d'utilisateurs reçoit les mêmes droits. Le nombre de groupes d'utilisateurs et leurs droits utilisateur peuvent être définis librement. Dans Data Protector, on distingue trois groupes d'utilisateurs par défaut : Administrateur, Opérateur et Utilisateur.

HP ITO
Voir **OVO**.

HP OpC
Voir **OVO**.

HP OpenView SMART Plug-In (SPI)
Solution entièrement intégrée et prête à l'emploi qui vient compléter HP OpenView Operations, élargissant ainsi le domaine géré. Grâce à l'intégration Data Protector, laquelle est mise en œuvre sous la forme d'un module HP OpenView SMART Plug-In, un utilisateur peut disposer d'un nombre arbitraire de Gestionnaire de cellule Data Protector considéré comme une extension de HP OpenView Operations (OVO).

HP OVO
Voir **OVO**.

HP VPO
Voir **OVO**.

ICDA *(terme spécifique à EMC Symmetrix)*
ICDA (Integrated Cached Disk Arrays) d'EMC est un périphérique à baie de disques combinant un ensemble de disques physiques, un certain nombre de canaux FWD SCSI, une mémoire cache interne et un logiciel de contrôle et de diagnostic communément appelé "microcode".

ID de connexion *(terme spécifique à MS SQL Server)*
Nom sous lequel un utilisateur se connecte à Microsoft SQL Server. Pour qu'un ID de connexion soit reconnu, une entrée doit avoir été créée pour l'utilisateur associé dans la table système syslogin de Microsoft SQL Server.

ID de session
Identificateur d'une sauvegarde, restauration, copie d'objet ou session de gestion de supports, composé de la date d'exécution de la session suivie d'un nombre unique.

ID de support
Identificateur unique attribué à un support par Data Protector.

ID d'objet *(terme spécifique à Windows)*
Les ID d'objet (OID) permettent d'accéder aux fichiers NTFS 5, quel que soit l'emplacement de ces derniers au sein du système. Data Protector considère les OID comme des flux de fichiers.

ID sauvegarde
L'identificateur d'un objet d'intégration qui est similaire à l'ID de session de la sauvegarde de l'objet en question. L'ID sauvegarde est conservé en cas de copie, exportation ou importation de l'objet.

IDB
Base de données interne de Data Protector, située sur le Gestionnaire de cellule, qui permet d'identifier les données sauvegardées, le type de support, la façon dont les sessions de sauvegarde et de restauration doivent se dérouler, ainsi que les périphériques et bibliothèques configurés.

image DR
Données requises pour l'installation et la configuration temporaires du système d'exploitation pour récupération après sinistre (DR OS).

importation de supports
Procédé consistant à relire dans la base de données IDB l'ensemble des données relatives aux sessions de sauvegarde qui se trouvent sur le support. Ceci permet

ensuite à l'utilisateur d'accéder rapidement et facilement aux données stockées sur les supports.
Voir aussi **exportation de supports.**

index de lecteur
Numéro permettant d'identifier la position mécanique d'un lecteur au sein d'une bibliothèque. Le contrôle robotique utilise ce numéro pour accéder à un lecteur.

Inet
Processus s'exécutant sur chaque système UNIX ou service s'exécutant sur chaque système Windows dans la cellule Data Protector. Il est responsable de la communication entre les systèmes de la cellule et du lancement des processus requis pour la sauvegarde et la restauration. Le service Inet est lancé dès que Data Protector est installé sur un système. Le processus Inet est démarré par le démon inetd.

informations de connexion à la base de données cible Oracle *(terme spécifique à Oracle et SAP R/3)*
Le format des informations de connexion est le suivant : <nom_utilisateur>/<mot de passe>@<service>, où :

- <nom_utilisateur> est le nom sous lequel un utilisateur est reconnu par le serveur Oracle et par les autres utilisateurs. Chaque nom d'utilisateur est associé à un mot de passe ; l'utilisateur doit les entrer tous les deux pour pouvoir se connecter à une base de données cible Oracle. Il doit également disposer de droits SYSDBA ou SYSOPER Oracle.

- <mot de passe> est une chaîne de caractères utilisée à des fins de protection des données et connue de l'utilisateur seul. Les utilisateurs doivent entrer un mot de passe pour pouvoir se connecter à un système d'exploitation ou à une application logicielle. Ce mot de passe doit correspondre à celui figurant dans le fichier de mots de passe Oracle (fichier orapwd) ; ce fichier permet d'authentifier les utilisateurs chargés de l'administration de la base de données.

- <service> est le nom servant à identifier un processus de serveur SQL*Net pour la base de données cible.

informations de connexion à la base de données du catalogue de récupération *(terme spécifique à Oracle)*
Le format des informations de connexion à la base de données du catalogue de récupération (Oracle) est le suivant : <nom_utilisateur>/<mot de passe>@<service>, où la description du

nom d'utilisateur, du mot de passe et du nom du service est la même que celle qui figure dans les informations de connexion SQL*Net V2 à la base de données cible Oracle. Dans ce cas, le <service> correspond au nom du service de la base de données catalogue de récupération et non à la base de données cible Oracle.

Remarque : l'utilisateur Oracle spécifié doit être le propriétaire du catalogue de récupération (Oracle).

initialisation
Voir **formatage**.

instance Oracle *(terme spécifique à Oracle*)
Chaque installation de base de données Oracle sur un ou plusieurs systèmes. Plusieurs instances de base de données peuvent s'exécuter sur un même système informatique.

interface de ligne de commande EMC Symmetrix (SYMCLI) *(terme spécifique à EMC Symmetrix)*
Voir **interface de ligne de commande Symmetrix (SYMCLI)**

interface de ligne de commande Symmetrix (SYMCLI) *(terme spécifique à EMC Symmetrix)*
Application développée à l'aide de l'interface de programmation d'applications Symmetrix (SYMAPI) qui récupère des données depuis une unité EMC Symmetrix utilisant certaines commandes SCSI de bas niveau. L'interface SYMCLI permet d'exécuter des commandes sur le système client afin d'obtenir des informations sur la configuration, l'état et les performances des unités EMC Symmetrix reliées à des clients évoluant dans un environnement ouvert.

interface de ligne de commande
Ensemble de commandes de type DOS et UNIX qui peuvent être utilisées dans les scripts shell pour effectuer des tâches de configuration, de sauvegarde, de restauration et de gestion dans Data Protector.

interface de périphérique virtuel

(terme spécifique à MS SQL Server 7.0/ 2000)
Interface de programmation de SQL Server 7.0/2000 permettant de sauvegarder et de restaurer rapidement des bases de données volumineuses.

interface de programmation d'applications EMC Symmetrix (SYMAPI) *(terme spécifique à EMC Symmetrix)*
Voir **interface de programmation d'applications Symmetrix (SYMAPI, Symmetrix Application Programming Interface)**

interface graphique utilisateur (GUI)
Interface graphique utilisateur interplate-forme (HP-UX, Solaris et Windows) fournie par Data Protector pour offrir un accès aisé à l'ensemble des tâches de configuration, d'administration et d'utilisation.

interface XBSA *(terme spécifique à Informix)*
L'utilitaire onbar et Data Protector communiquent par le biais de l'interface XBSA (X/Open Backup Specification Services Programmer's Interface).

Internet Information Server (IIS)

(terme spécifique à Windows)
Microsoft Internet Information Server est un fichier réseau et un serveur d'applications qui prend en charge de nombreux protocoles. La fonction principale d'IIS consiste à transmettre les informations des pages HTML (Hypertext Markup Language) à l'aide du protocole HTTP (Hypertext Transport Protocol).

ISQL *(terme spécifique à Sybase)*
Utilitaire Sybase servant à effectuer des tâches d'administration système sur Sybase SQL Server.

ITO
Voir **OVO**.

jeu de copies miroir *(terme spécifique à MS VSS)*
Ensemble de copies miroir créées au même instant.
Voir aussi **copie miroir.**

jeu de disquettes ASR
Ensemble de fichiers stockés sur plusieurs disquettes, nécessaires pour la reconfiguration appropriée du disque de rechange (partition du disque et configuration des volumes logiques), ainsi que pour la récupération automatique du système d'origine et des données utilisateur sauvegardées lors de la sauvegarde complète du client.
Ces fichiers sont stockés comme fichier archive ASR sur le Gestionnaire de cellule (dans <*répertoire_Data_Protector*>\Config\Server\dr\asr sur un Gestionnaire de cellule Windows ou dans /etc/opt/omni/server/dr/asr/ sur un Gestionnaire de cellule UNIX) ainsi que sur le support de sauvegarde Le fichier archive ASR est extrait sur trois disquettes sur les systèmes Windows 32 bits, ou sur quatre disquettes sur les systèmes Windows 64 bits lorsqu'un sinistre a eu lieu. Ces disquettes sont nécessaires pour effectuer l'ASR.

jeu de répliques *(terme spécifique à ZBD)*
Un groupe de répliques, toutes créées en utilisant la même spécification de

sauvegarde.
Voir aussi **réplique** et **rotation du jeu de répliques**.

jeu de sauvegardes
Un jeu complet d'objets d'intégration associés à une sauvegarde.

jeu de sauvegardes *(terme spécifique à Oracle)*
Regroupement logique de fichiers sauvegardés créés à l'aide de la commande de sauvegarde RMAN. Un jeu de sauvegardes est un ensemble complet de fichiers associés à une sauvegarde. Pour améliorer les performances, les fichiers peuvent être multiplexés. Un jeu de sauvegardes contient soit des fichiers de données soit des journaux d'archive, mais non les deux à la fois.

jeu de supports
Une session de sauvegarde a pour résultat le stockage de données sur un groupe de supports appelé "jeu de supports". Selon la stratégie d'utilisation des supports, plusieurs sessions peuvent se partager les mêmes supports.

jonction de répertoires *(terme spécifique à Windows)*
Les jonctions de répertoires utilisent le concept de point d'analyse de Windows. Une jonction de répertoire NTFS 5 permet à l'utilisateur de rediriger une requête de répertoire/fichier vers un autre emplacement.

journal d'événements Data Protector
Référentiel central de l'ensemble des notifications ayant trait à Data Protector. Par défaut, toutes les notifications sont envoyées au journal d'événements. Ce dernier n'est accessible qu'aux utilisateurs Data Protector appartenant au groupe Admin et à ceux qui disposent des droits utilisateur Rapports et notifications. Vous pouvez afficher ou supprimer l'ensemble des événements du journal.

journal de rétablissement archivé

(terme spécifique à Oracle)
Egalement appelé journal de rétablissement hors ligne. Si la base de données Oracle fonctionne en mode ARCHIVELOG, chaque journal de rétablissement en ligne, lorsqu'il est plein, est copié dans un (ou plusieurs) emplacement(s) de destination des journaux archivés. Cette copie est appelée Journal de rétablissement archivé. La présence ou l'absence de ce journal dépend du mode de fonctionnement de la base de données :

- ARCHIVELOG - Les fichiers journaux de rétablissement en ligne, une fois pleins, sont archivés avant d'être réutilisés. La base de données

peut être récupérée à partir d'une défaillance de disque ou d'instance. Vous ne pouvez effectuer de sauvegarde "à chaud" que si la base de données fonctionne dans ce mode.

- NOARCHIVELOG - Les fichiers journaux de rétablissement en ligne ne sont pas archivés.

Voir aussi **journal de rétablissement en ligne.**

journal de rétablissement en ligne *Voir* **journal de rétablissement archivé**.

journal de rétablissement en ligne

(terme spécifique à Oracle)
Journaux de rétablissement qui n'ont pas été archivés, mais qui sont à la disposition de l'instance à des fins d'enregistrement de la base de données ou qui sont pleins et attendent d'être archivés ou réutilisés.
Voir aussi **journal de rétablissement archivé**.

journal de rétablissement *(terme spécifique à Oracle)*
Chaque base de données Oracle dispose d'un ensemble de plusieurs fichiers journaux de rétablissement. Cet ensemble est appelé "journal de rétablissement de la base de données". Oracle y consigne toutes les modifications apportées aux données.

journaux de transactions (*Data Protector terme spécifique à)*
Assure le suivi des modifications de la base de données IDB. Il est recommandé d'activer l'archivage des journaux de transactions pour éviter de perdre les fichiers journaux créés après la dernière sauvegarde de la base de données IDB et nécessaires à sa récupération.

journaux d'événements
Fichiers dans lesquels Windows enregistre tous les événements, tels que le démarrage et l'interruption des services, et les connexions et déconnexions des utilisateurs. Data Protector peut sauvegarder les journaux d'événements Windows dans le cadre de la sauvegarde de la configuration Windows.

LDEV HP StorageWorks Disk Array XP
Partition logique d'un disque physique dans une baie de disques HP StorageWorks Disk Array XP. Les LDEV sont des entités qui peuvent être dupliquées dans les configurations Continuous Access XP (CA) et Business Copy XP (BC) ou bien utilisées en tant qu'entités autonomes.
Voir aussi **BC** *(terme spécifique à*

HP StorageWorks Disk Array XP), **CA** *(terme spécifique à HP StorageWorks Disk Array XP)* et **réplique**.

lecteur
Unité physique recevant des données provenant d'un système informatique et capable de les écrire sur un support magnétique (généralement un lecteur de bande). Un lecteur peut également lire les données du support et les envoyer au système informatique.

liste de préallocation
Dans un pool de supports, sous-ensemble de supports définissant l'ordre dans lequel les supports sont utilisés pour la sauvegarde.

LISTENER.ORA *(terme spécifique à Oracle)*
Fichier de configuration Oracle décrivant un ou plusieurs listeners TNS (Transparent Network Substrate) sur un serveur.

LUN HP StorageWorks Virtual Array
Partition logique d'un disque physique dans une baie de virtualisation HP StorageWorks Virtual Array. Les LUN sont des entités qui peuvent être dupliquées dans la configuration HP StorageWorks Business Copy VA ou bien utilisées en tant qu'entités autonomes.
Voir aussi **BC VA** et **réplique**.

LVM
Un LVM (Logical Volume Manager), ou gestionnaire de volume logique, est un sous-système permettant de structurer l'espace disque physique et de le mettre en correspondance avec les volumes logiques sur les systèmes UNIX. Un système LVM est constitué de plusieurs groupes de volumes, comportant chacun plusieurs volumes.

Manager-of-Managers (MoM)
Voir **Entreprise Gestionnaire de cellule**.

MAPI *terme spécifique à Microsoft Exchange)*
L'interface MAPI (Messaging Application Programming Interface) est l'interface de programmation qui permet aux applications et aux clients de messagerie communiquer avec les systèmes de messagerie et d'information.

MFS
Le MFS (Migrating File System), ou système de fichiers migrant, met des fonctions de migration à la disposition d'un système de fichiers JFS standard (sur HP-UX 11.00). Il est accessible via une interface de système de fichiers standard (DMAPI), et se monte sur un répertoire comme n'importe quel système de fichiers HP-UX. Dans un MFS, seules les informations de superblock, d'inode et d'attribut étendu

demeurent en permanence sur le disque dur et ne migrent jamais.
Voir aussi **VBFS**.

Microsoft Exchange Server
Système de messagerie "client-serveur" et de groupes de travail fournissant une connexion transparente à de nombreux systèmes de communication différents. Il offre aux utilisateurs un système de messagerie électronique, une solution de planification de groupe et individuelle, des formulaires en ligne et des outils d'automatisation du flux de travail. Il fournit également au développeur une plate-forme sur laquelle il peut élaborer des applications personnalisées de partage d'informations et de service de messagerie.

Microsoft Management Console (MMC) *(terme spécifique à Windows)*
Modèle d'administration pour environnements Windows. Cette console met à votre disposition une interface utilisateur d'administration simple, cohérente et intégrée permettant de gérer de nombreuses applications à partir d'une seule et même interface, à condition toutefois que les applications soient compatibles avec le modèle MMC.

Microsoft SQL Server 7.0/2000
Système de gestion de base de données conçu pour répondre aux besoins du traitement distribué "client-serveur".

miroir *(terme spécifique à EMC Symmetrix et HP StorageWorks Disk Array XP)*
Voir **volume cible**.

miroir de premier niveau (*terme spécifique à HP StorageWorks Disk Array XP*)
HP StorageWorks Disk Array XP peut comporter jusqu'à trois copies miroir d'un volume principal, chacune d'entre elles pouvant également posséder deux copies supplémentaires. Les trois copies miroir sont appelées miroirs de premier niveau.
Voir également **Volume principal** et **numéros de MU**.

miroir d'objet
Copie d'un objet sauvegarde créé à l'aide de la mise en miroir d'objet. Les miroirs d'objet sont souvent appelés copies d'objet.

mise au coffre de supports
Procédé consistant à stocker des supports dans un emplacement sécurisé et distant. Les supports sont retournés au "centre de données" lorsqu'une restauration de données est nécessaire ou lorsqu'ils sont prêts à être réutilisés pour d'autres sauvegardes. La façon dont la mise au coffre est réalisée dépend de la stratégie de sauvegarde adoptée par votre entreprise et de sa politique de protection et de fiabilité de données.

mise en miroir d'objet
Processus consistant à écrire les mêmes données sur plusieurs jeux de supports au cours d'une session de sauvegarde. Data Protector vous permet de mettre en miroir tous les objets sauvegarde ou certains seulement sur un ou plusieurs jeux de supports.

MMD
Le processus (service) MMD (Media Management Daemon), ou démon de gestion des supports, s'exécute sur le Gestionnaire de cellule Data Protector et contrôle les opérations relatives aux périphériques et à la gestion des supports. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.

MMDB
La base de données de gestion des supports (MMDB) fait partie de la base de données IDB, laquelle contient les informations concernant les supports, les pools de supports, les périphériques, les bibliothèques, les lecteurs de bibliothèques et les emplacements configurés dans la cellule, ainsi que les supports Data Protector utilisés pour la sauvegarde. Dans un environnement de sauvegarde d'entreprise, cette partie de la base de données peut être commune à toutes les cellules.
Voir aussi **CMMDB**, **CDB**.

module d'écriture *(terme spécifique à MS VSS)*
Processus initiant la modification des données sur le volume d'origine. Les modules d'écriture sont généralement des applications ou des services système rédigeant des informations permanentes sur un volume. Ils participent également au processus de synchronisation des copies miroir en assurant la cohérence des données.

MoM
Plusieurs cellules peuvent être regroupées et gérées depuis une cellule centrale. Le système de gestion de la cellule centrale est le Manager-of-Managers (MoM). Celui-ci permet à l'utilisateur de configurer et de gérer plusieurs cellules à partir d'un point central.

moteur de stockage extensible (ESE, pour Extensible Storage Engine)

(terme spécifique à Microsoft Exchange Server 2000/2003)
Technologie de base de données utilisée comme système de stockage pour les échanges d'informations dans Microsoft Exchange Server 2000/2003.

moteur XCopy *(terme spécifique à la sauvegarde directe)*
Commande SCSI-3 permettant de copier des données d'un périphérique de stockage doté d'une adresse SCSI

source vers un périphérique de stockage doté d'une adresse SCSI cible, autorisant ainsi une sauvegarde directe. Les données transitent du périphérique source (en bloc ou en continu, c'est-à-dire sur disque ou sur bande) vers le périphérique cible (en bloc ou en continu) via XCopy. Ainsi, le serveur de contrôle n'a plus besoin de transférer les données du périphérique de stockage vers la mémoire ni de les écrire sur le périphérique cible.
Voir aussi **sauvegarde directe**.

MSM
Le Gestionnaire de session de supports (Media Session Manager) de Data Protector s'exécute sur le Gestionnaire de cellule et régit les sessions de supports, telles que la copie de supports.

niveau de journalisation
Le niveau de journalisation indique le nombre de détails concernant les fichiers et répertoires qui sont écrits dans la base de données IDB pendant la sauvegarde ou la copie d'objets. Vous pouvez toujours restaurer vos données, sans tenir compte du niveau de journalisation utilisé pendant la sauvegarde. Data Protector propose quatre niveaux de journalisation : Journaliser tout, Journaliser répertoires, Journaliser fichiers, Pas de journalisation. Les différents paramètres de niveau de journalisation influencent la croissance de la base de données IDB, la vitesse de sauvegarde et la facilité d'exploration des données à restaurer.

nom de verrouillage
Vous pouvez configurer plusieurs fois le même périphérique physique avec des caractéristiques différentes en utilisant des noms de périphérique distincts.

Le nom de verrouillage est une chaîne spécifiée par l'utilisateur servant à verrouiller toute configuration de périphérique de ce type afin d'empêcher un conflit si plusieurs de ces périphériques (noms de périphériques) sont utilisés simultanément. Utilisez un nom de verrouillage identique pour toutes les définitions de périphériques utilisant le même périphérique physique.

numéro de MU (*terme spécifique à HP StorageWorks Disk Array XP*)
Chiffre entier (0, 1 ou 2) servant à indiquer qu'il s'agit d'un miroir de premier niveau.
Voir aussi **miroir de premier niveau**.

obdrindex.dat
Base de données IDB stockant des informations sur les sauvegardes IDB, les périphériques et les supports utilisés pour la sauvegarde. Ces données peuvent simplifier considérablement la récupération de la base de données IDB. Il est recommandé de déplacer le fichier, ainsi que les journaux de transactions de

la base de données IDB, sur un disque physique séparé des autres répertoires de la base IDB, mais aussi de faire une copie du fichier et de la mettre à l'emplacement de votre choix.

objet d'intégration
Un objet sauvegarde d'une intégration de Data Protector, telle que Oracle ou SAP DB.

objet sauvegarde
Unité de sauvegarde contenant tous les éléments sauvegardés d'un volume de disque (disque logique ou point de montage). Les éléments sauvegardés peuvent être des fichiers, des répertoires ou l'ensemble du disque ou du point de montage. En outre, un objet sauvegarde peut être une entité de base de données ou une image disque (rawdisk).

Un objet sauvegarde est défini comme suit :

- Nom de client : nom d'hôte du client Data Protector dans lequel l'objet sauvegarde est hébergé.
- Point de montage : point d'accès dans une structure de répertoires (lecteur sous Windows et point de montage sous UNIX) sur le client contenant l'objet sauvegarde.
- Description: définit exclusivement les objets sauvegarde avec un nom de client et un point de montage identiques.
- Saisissez : type d'objet sauvegarde (par exemple, un système de fichier ou Oracle).

objet
Voir **objet sauvegarde**

OmniStorage
Logiciel permettant d'effectuer une migration transparente des données les moins utilisées vers la bibliothèque optique et de conserver les plus utilisées sur le disque dur. HP OmniStorage fonctionne sur les systèmes HP-UX.

ON-Bar *(terme spécifique à Informix)*
Système de sauvegarde et de restauration du serveur en ligne. ON-Bar permet à l'utilisateur de créer une copie des données stockées sur son serveur en ligne et de les restaurer ultérieurement. Le système de sauvegarde et de restauration ON-Bar nécessite l'intervention des composants suivants :

- Utilitaire onbar
- Data Protector (en tant que solution de sauvegarde)
- Interface XBSA

- tables de catalogue ON-Bar servant à sauvegarder les dbobjects et à effectuer un suivi des instances de dbobjects dans plusieurs sauvegardes.

ONCONFIG *(terme spécifique à Informix)*
Variable d'environnement spécifiant le nom du fichier de configuration ONCONFIG actif. En cas d'absence de la variable d'environnement ONCONFIG, les valeurs de configuration du fichier <*INFORMIXDIR*>\etc\onconfig (sur les systèmes HP-UX) ou <*INFORMIXDIR*>/etc/onconfig (sur les systèmes Windows) sont utilisées.

OpC
Voir **OVO**.

opérateurs booléens
Les opérateurs booléens pour la fonction de recherche sur le texte entier du système d'aide en ligne sont AND, OR, NOT et NEAR (ET, OU, NON et PROCHE). Utilisés lors d'une recherche, ils vous permettent de définir précisément votre requête en établissant une relation entre les termes de la recherche. AND est utilisé par défaut lorsque vous ne spécifiez aucun opérateur dans une recherche avec plusieurs termes. Par exemple, la requête récupération après sinistre manuelle équivaut à récupération AND (ET) après AND (ET) sinistre AND (ET) manuelle.

opération hors contrôle ou **opération sans surveillance**
Sauvegarde ou restauration ayant lieu en dehors des heures normales de bureau, ce qui signifie qu'aucun opérateur n'est présent pour utiliser l'application de sauvegarde ou les demandes de montage de service, par exemple.

opération sans surveillance
Voir **opération hors contrôle**.

ORACLE_SID *(terme spécifique à Oracle)*
Nom unique pour une instance de serveur Oracle. Pour passer d'un serveur Oracle à un autre, spécifiez le <*ORACLE_SID*> voulu. Le <*ORACLE_SID*> est inséré dans les parties CONNECT DATA du descripteur de connexion d'un fichier TNSNAMES.ORA et dans la définition du listener TNS du fichier LISTENER.ORA.

OVO
HP OpenView Operations pour Unix offre des fonctions puissantes pour gérer les opérations d'un grand nombre de systèmes et d'applications à l'intérieur d'un réseau. Data Protector fournit une intégration de ce produit de gestion. Cette intégration est mise en œuvre sous

la forme d'un module SMART Plug-In pour les serveurs de gestion OVO sous HP-UX et Solaris. Les versions antérieures d'OVO se nommaient IT/ Operation, Operations Center et Vantage Point Operations.
Voir aussi **fusion**.

package *(terme spécifique à MC/ ServiceGuard et à Veritas Cluster)*
Ensemble de ressources (groupes de volumes, services d'applications, noms et adresses IP, par exemple) nécessaires à l'exécution d'une application compatible cluster spécifique.

paquet magique
Voir **Wake ONLAN**.

parallélisme
Concept consistant à lire plusieurs flux de données depuis une base de données en ligne.

parallélisme de bases de données
Plusieurs bases de données sont sauvegardées simultanément si le nombre de périphériques disponibles permet d'effectuer des sauvegardes en parallèle.

partage de charge
Par défaut, Data Protector équilibre automatiquement la charge (l'utilisation) des périphériques sélectionnés pour la sauvegarde, afin que ces derniers soient utilisés de manière uniforme. Ce procédé permet d'optimiser l'utilisation des périphériques en équilibrant le nombre des objets écrits sur chacun. Cette opération s'effectuant automatiquement pendant la sauvegarde, l'utilisateur n'a pas besoin de gérer la sauvegarde des données ; il lui suffit de spécifier les périphériques à utiliser. Si vous ne souhaitez pas utiliser l'équilibrage de charge, vous pouvez sélectionner le périphérique à utiliser avec chaque objet dans le spécification de sauvegarde. Data Protector accèdera aux périphériques dans l'ordre spécifié.

partition système
Partition contenant les fichiers du système d'exploitation. La terminologie utilisée par Microsoft définit la partition système comme une partition contenant les fichiers nécessaires pour assurer les premières étapes du processus d'amorçage.

passage
Voir **basculement**

périphérique
Unité physique contenant soit un lecteur, soit une unité plus complexe (une bibliothèque par exemple).

périphérique cible (R2) *(terme spécifique à EMC Symmetrix)*
Périphérique EMC Symmetrix prenant part aux opérations SRDF avec un

périphérique source (R1). Il réside sur l'unité EMC Symmetrix distante. Il est apparié à un périphérique source (R1) dans l'unité EMC Symmetrix locale et reçoit toutes les données écrites sur le périphérique dont il est le miroir. Pendant les opérations d'E/S courantes, les applications utilisateur ne peuvent accéder à ce périphérique cible. Tout périphérique R2 doit être affecté à un type de groupe RDF2.
Voir aussi **périphérique source (R1)**

périphérique compatible OBDR
Périphérique capable d'émuler un lecteur de CD-ROM contenant un disque amorçable et pouvant donc servir de périphérique de sauvegarde ou d'amorçage à des fins de récupération après sinistre.

périphérique de bibliothèque de fichiers
Périphérique résidant sur un disque émulant une bibliothèque contenant plusieurs supports, donc plusieurs fichiers ; désigné sous le terme dépôts de fichier.

périphérique de bibliothèque de stockage
Périphérique composé de plusieurs emplacements destinés à stocker des supports optiques ou des fichiers. Lorsqu'il est utilisé pour le stockage de fichiers, le périphérique de bibliothèque de stockage est appelé "périphérique de bibliothèque de stockage de fichiers".

périphérique de bibliothèque de stockage de fichiers
Périphérique situé sur un disque se composant de plusieurs emplacements destinés au stockage des fichiers.

périphérique de fichier autonome
Un périphérique de fichier est un fichier situé dans un répertoire spécifié dans lequel vous sauvegardez des données.

périphérique de sauvegarde
Périphérique configuré pour une utilisation avec Data Protector, capable d'écrire et de lire des données sur un support de stockage. Il peut s'agir, par exemple, d'un lecteur DDS/DAT autonome ou d'une bibliothèque.

périphérique en mode continu
On dit d'un périphérique qu'il fonctionne en mode continu s'il peut fournir un volume de données suffisant au support pour que ce dernier fonctionne en continu. Dans le cas contraire, l'avancement de la bande doit être interrompu, le périphérique attend d'avoir reçu d'autres données, fait légèrement reculer la bande, puis reprend l'écriture des données, et ainsi de suite. En d'autres termes, si le taux auquel les données sont écrites sur la bande est inférieur ou égal à celui

auquel elles sont fournies au périphérique par le système informatique, le périphérique fonctionne en mode continu. Ce procédé améliore considérablement les performances du périphérique et la gestion de l'espace de stockage.

périphérique physique
Unité physique contenant soit un lecteur, soit une unité plus complexe (une bibliothèque, par exemple).

périphérique source (R1) *(terme spécifique à EMC Symmetrix)*
Périphérique EMC Symmetrix prenant part aux opérations SRDF avec un périphérique cible (R2). Toutes les données écrites sur ce périphérique sont mises en miroir sur un périphérique cible (R2) situé sur une unité EMC Symmetrix distante. Tout périphérique R1 doit être attribué à un type de groupe RDF1.
Voir aussi **périphérique cible (R2)**.

planificateur
Fonction permettant de contrôler le moment et la fréquence des sauvegardes automatiques. En définissant un calendrier, l'utilisateur peut automatiser le lancement des sauvegardes.

point d'analyse *(terme spécifique à Windows)*
Attribut contrôlé par le système et pouvant être associé à tout répertoire ou fichier. La valeur d'un attribut d'analyse peut avoir des données définies par l'utilisateur. Le format des données est reconnu par l'application sur laquelle elles étaient stockées et par un filtre de système de fichiers installé dans le but de permettre l'interprétation des données et le traitement des fichiers. Chaque fois que le système de fichiers rencontre un fichier comportant un point d'analyse, il essaie de trouver le filtre de système de fichiers associé au format de données.

point de montage
Point d'accès à un disque ou à un volume logique dans une structure de répertoires, par exemple /opt ou d:. Sous UNIX, les points de montage sont accessibles au moyen de la commande bdf ou df.

point de montage de volume (*terme spécifique à Windows*)
Répertoire vide sur un volume pouvant être utilisé pour le montage d'un autre volume. Le point de montage de volume sert de passerelle vers le volume cible. Une fois le volume monté, les utilisateurs et les applications peuvent consulter les données stockées sur celui-ci par le chemin d'accès au système de fichiers complet (fusionné), comme si les deux volumes ne faisaient qu'un.

pont FC
Voir **pont Fibre Channel**

pont Fibre Channel
Un pont ou multiplexeur Fibre Channel permet de réaliser une migration des périphériques SCSI parallèles existants, tels que les baies de disques RAID, les disques SSD et les bibliothèques de bandes vers un environnement Fibre Channel. Une interface Fibre Channel se trouve à une extrémité du pont ou multiplexeur. Des ports SCSI parallèles se trouvent à l'autre extrémité. Le pont ou multiplexeur permet de déplacer les paquets SCSI entre les périphériques Fibre Channel et SCSI parallèles.

pool de supports
Ensemble de supports du même type (DDS par exemple), utilisé et suivi comme un groupe. Les supports sont formatés et attribués à un pool.

pool libre
Source auxiliaire de supports utilisée par les pools n'ayant plus aucun support disponible. Les pools de supports doivent être configurés pour l'utilisation de pools libres.

post-exécution
Option de sauvegarde qui exécute une commande ou un script après la sauvegarde d'un objet ou une fois que la session de sauvegarde est terminée. Les commandes de post-exécution ne sont pas fournies avec Data Protector. L'utilisateur doit les créer lui-même. Elles peuvent être rédigées sous la forme de programmes exécutables ou de fichiers séquentiels sous Windows, ou bien de scripts shell sous UNIX.
Voir aussi **pré-exécution**.

pré-exécution
Option de sauvegarde qui exécute une commande ou un script avant la sauvegarde d'un objet ou avant que la session de sauvegarde ne démarre. Les commandes de pré-exécution ne sont pas fournies avec Data Protector. L'utilisateur doit les créer lui-même. Elles peuvent être rédigées sous la forme de programmes exécutables ou de fichiers séquentiels sous Windows, ou bien de scripts shell sous UNIX.
Voir aussi **post-exécution**.

processus BC *(terme spécifique à EMC Symmetrix)*
Solution d'environnement de stockage protégé dans le cadre de laquelle des périphériques EMC Symmetrix ont été spécialement configurés en tant que miroirs ou volumes de continuité d'activité pour protéger les données stockées sur des périphériques EMC Symmetrix standard.
Voir aussi **BCV**.

processus de copie d'objet
Processus de copie des versions d'objet sélectionnées sur un jeu de supports spécifique. Vous pouvez sélectionner pour la copie des versions d'objet d'une ou de plusieurs sessions de sauvegarde.

profil utilisateur *(terme spécifique à Windows)*
Informations de configuration définies pour chaque utilisateur. Ces informations comprennent la configuration du bureau, les couleurs d'écran sélectionnées, les connexions réseau, etc. Lorsqu'un utilisateur se connecte, le système charge son profil et l'environnement Windows le prend en compte.

propriétaire de la sauvegarde
Tout objet sauvegarde de la base de données IDB a un propriétaire. Par défaut, il s'agit de l'utilisateur qui a lancé la session de sauvegarde.

propriété
La propriété d'une sauvegarde détermine qui est autorisé à restaurer des fichiers à partir de la sauvegarde. Le propriétaire de la session est la personne qui démarre la sauvegarde interactive. Si un utilisateur démarre une spécification de sauvegarde existante sans la modifier, la session n'est pas considérée comme interactive. Dans ce cas, si le propriétaire de la sauvegarde a été défini dans la spécification de la sauvegarde, celui-ci reste le propriétaire de la session. Dans le cas contraire, le propriétaire de la session est l'utilisateur qui a démarré la sauvegarde concernée. Pour les sauvegardes planifiées, le propriétaire par défaut de la session pour le Gestionnaire de cellule Unix est root.sys@<Gestionnaire de cellule>. Pour le Gestionnaire de cellule Windows, il s'agira de l'utilisateur indiqué pendant l'installation du Gestionnaire de cellule. Il est possible de modifier la propriété de manière à ce qu'un utilisateur spécifique devienne le propriétaire de la session.

protection
Voir **protection de données** et **protection de catalogue**.

protection de catalogue
Permet de définir le temps de conservation des informations concernant les données sauvegardées (sauvegarde, noms et versions de fichiers) dans la base de données IDB. *Voir aussi* **protection de données**.

protection de données
Permet de définir le délai de protection des données sauvegardées sur un support, c'est-à-dire la durée pendant laquelle Data Protector ne peut les écraser. Une fois ce délai expiré, Data Protector peut réutiliser le support lors d'une prochaine session de sauvegarde. *Voir aussi* **protection de catalogue**.

pulsation
Ensemble de données de cluster qui comporte un horodatage contenant des informations sur l'état de

fonctionnement d'un nœud de cluster spécifique. Cet ensemble de données est distribué à tous les nœuds de cluster.

quota de disque
Concept permettant de gérer l'utilisation de l'espace disque pour l'ensemble des utilisateurs ou pour certains d'entre eux sur un système informatique. Plusieurs plates-formes de système d'exploitation utilisent ce concept.

quotas de disque utilisateur
Le support de gestion des quotas NTFS permet le contrôle et le suivi élaboré de l'utilisation de l'espace disque sur les volumes de stockage partagés. Data Protector sauvegarde des quotas de disque utilisateur sur l'ensemble du système et pour tous les utilisateurs configurés à un instant donné.

RAID
Redundant Array of Inexpensive Disks, baie de disques durs redondants bon marché.

RCU *(terme spécifique à HP StorageWorks)*
Unité agissant comme esclave d'une MCU dans une configuration CA. Dans les configurations bidirectionnelles, la RCU peut également agir comme une MCU.

RDF1/RDF2 *(terme spécifique à EMC Symmetrix)*
Type de groupe de périphériques SRDF. Seuls les périphériques RDF peuvent être attribués à un groupe RDF. Le type de groupe RDF1 contient des périphériques sources (R1) et le type de groupe RDF2 des périphériques cibles (R2).

RDS
Le processus RDS (Raima Database Server) s'exécute sur le Gestionnaire de cellule Data Protector et gère la base de données IDB. Le processus démarre dès que Data Protector est installé sur le Gestionnaire de cellule.

RecoveryInfo
Lors de la sauvegarde de fichiers de configuration Windows, Data Protector collecte les informations sur la configuration système actuelle (volume, configuration disque et réseau) Ces informations sont nécessaires pour la récupération après sinistre.

récupération après sinistre
Procédé permettant de restaurer le disque du système principal d'un client dans un état proche de celui dans lequel il se trouvait après une sauvegarde complète.

récupération hors ligne
Une récupération hors ligne s'effectue lorsque le Gestionnaire de cellule n'est

pas accessible (en raison de problèmes sur le réseau, par exemple). Seuls les périphériques autonomes et les périphériques de bibliothèque SCSI peuvent être utilisés pour une récupération hors ligne. La récupération du Gestionnaire de cellule s'effectue toujours hors ligne.

récupération matérielle *(terme spécifique à Microsoft Exchange Server)*
Récupération de la base de données Microsoft Exchange Server effectuée après une restauration par le moteur de base de données, au moyen des fichiers de journal des transactions.

recyclage
Processus consistant à supprimer la protection de toutes les données sauvegardées se trouvant sur le support, autorisant ainsi Data Protector à les écraser au cours de l'une des sauvegardes ultérieures. Les données provenant de la même session, mais se trouvant sur d'autres supports, ne sont plus protégées non plus. Le recyclage ne modifie pas les données qui se trouvent sur le support.

réécriture
Option définissant un mode de résolution de conflits pendant la restauration. Tous les fichiers sauvegardés sont restaurés, même s'ils sont plus anciens que les fichiers existants.
Voir aussi **fusion**.

registre Windows
Base de données centralisée utilisée par Windows pour stocker les informations relatives à la configuration du système d'exploitation et des applications installées.

répertoire DC
Le répertoire de catalogue des détails (DC) est constitué des fichiers binaires DC où sont stockées les informations relatives aux versions de fichier. Il constitue la partie DCBF de la base de données IDB dont il occupe environ 80 %. Le répertoire DC par défaut est intitulé dcbf et se trouve dans le répertoire *<répertoire_Data_Protector>*\db40 sur un Gestionnaire de cellule Windows et dans le répertoire /var/opt/omni/server/db40 sur un Gestionnaire de cellule UNIX. Vous pouvez créer d'autres répertoires DC et les enregistrer à l'emplacement de votre choix. Chaque cellule peut gérer jusqu'à 10 répertoires DC. La taille maximale par défaut d'un répertoire DC est de 2 Go.

réplique *(terme spécifique à ZBD)*
Une image, à un instant T, des données des volumes source qui contiennent les objets sauvegarde spécifiques à l'utilisateur. En fonction du matériel/

logiciel avec lequel elle est créée, l'image peut être un doublon exact indépendant (clone) des blocs de stockage au niveau du disque physique (split mirror, par exemple) ou bien une copie virtuelle (par exemple, un snapshot). Du point de vue de l'hôte, sur un système de base UNIX ou Windows, le disque physique complet contenant l'objet sauvegarde est dupliqué. Toutefois, si un gestionnaire de volume est utilisé sur UNIX, le groupe entier de volumes/disques contenant un objet sauvegarde est dupliqué.
Voir aussi **snapshot**, **création de snapshot**, **split mirror** et **création de split mirror**.

restauration incrémentale *(terme spécifique à EMC Symmetrix)*
Opération de contrôle BCV ou SRDF. Dans les opérations de contrôle BCV, une restauration incrémentale réaffecte un périphérique BCV comme miroir disponible suivant du périphérique standard de la paire. Cependant, les périphériques standard sont mis à jour uniquement avec les données écrites sur le périphérique BCV au cours de la séparation des paires d'origine ; les données écrites sur le périphérique standard au cours de la séparation sont écrasées par les données du miroir BCV. Dans les opérations de contrôle SRDF, une restauration incrémentale réaffecte un périphérique (R2) cible comme miroir disponible suivant du périphérique (R1) source de la paire. Cependant, les périphériques (R1) source sont mis à jour uniquement avec les données écrites sur le périphérique (R2) cible au cours de la séparation des paires d'origine ; les données écrites sur le périphérique (R1) source au cours de la séparation sont écrasées par les données du miroir (R2) cible.

restauration instantanée (*(terme spécifique à ZBD*)
Processus par lequel une duplication effectuée lors d'une sauvegarde sur disque ou sur disque+bande permet de restaurer le contenu des volumes source tel qu'il était au moment de la création de la réplique, permettant ainsi de ne pas effectuer de restauration à partir de la bande. Suivant l'application/la base de données concernée, cela peut suffire. Dans d'autres cas, des étapes supplémentaires peuvent être requises en vue d'une récupération complète, l'application de journaux de transaction par exemple.
Voir aussi **réplique**, **sauvegarde avec temps d'indisponibilité nul (ZDB)**, **sauvegarde sur disque ZDB** et **ZDB sur disque + bande**.

récupération locale et distante
La récupération distante s'effectue lorsque tous les hôtes de l'Agent de support spécifiés dans le fichier SRD sont accessibles. Si l'un d'entre eux échoue, le processus de récupération

après sinistre bascule du mode distant au mode local. Dans ce cas, le système cible est parcouru pour la recherche de périphériques connectés en local. Si la recherche ne renvoie qu'un seul périphérique, celui-ci sera automatiquement utilisé. Dans le cas contraire, Data Protector vous invitera à sélectionner le périphérique à utiliser pour la restauration.

restauration parallèle
Procédé consistant à restaurer simultanément (c'est-à-dire en parallèle) des données sauvegardées vers plusieurs disques, en exécutant pour cela plusieurs Agents de disque qui reçoivent des données d'un Agent de support. Pour que la restauration parallèle fonctionne, les données sélectionnées doivent se trouver sur des disques ou volumes logiques différents, et lors de la sauvegarde, les données provenant des différents objets doivent avoir été envoyées au même périphérique avec deux Agents de disque ou plus. Pendant une restauration parallèle, les données concernant les différents objets à restaurer sont lues simultanément sur les supports, améliorant ainsi les performances du système.

restauration Split Mirror *(terme spécifique à EMC Symmetrix et HP StorageWorks Disk Array XP)*
Processus dans lequel les données sauvegardées lors d'une session de sauvegarde sur bande ou sur disque+bande avec temps d'indisponibilité nul sont restaurées du support de bande sur une réplique split mirror qui est alors synchronisée avec les volumes source. Les objets sauvegarde individuels ou les sessions complètes peuvent être restauré(e)s à l'aide de cette méthode.
Voir aussi **sauvegarde sur bande ZDB**, **ZDB sur disque + bande** et **réplique**.

RMAN *(terme spécifique à Oracle)*
Voir **gestionnaire de récupération**.

rotation des miroirs *(terme spécifique à HP StorageWorks Disk Array XP)*
Voir **rotation du jeu de répliques**.

rotation du jeu de répliques *(terme spécifique à ZBD)*
Utilisation d'un jeu de répliques pour la génération régulière de sauvegardes : Chaque fois qu'une même spécification de sauvegarde requiérant l'utilisation d'un jeu de répliques est exécutée, une nouvelle réplique est créée et ajoutée au jeu, jusqu'à obtention du nombre maximal de répliques pour le jeu. La réplique la plus ancienne du jeu est alors remplacée et le nombre maximal de répliques du jeu conservé.
Voir aussi **réplique** et **jeu de répliques**.

RSM
Le Restore Session Manager Data Protector (Gestionnaire de session de

restauration) contrôle la session de restauration. Ce processus est toujours exécuté sur le système du Gestionnaire de cellule.

RSM *(terme spécifique à Windows)*
Le RSM (Removable Storage Manager), ou Gestionnaire de supports amovibles, comprend un service de gestion des supports facilitant la communication entre les applications, les changeurs robotiques et les bibliothèques de supports. Il permet à plusieurs applications de partager des bibliothèques de supports robotiques locales et des lecteurs de disques ou de bandes, et de gérer les supports amovibles.

SAPDBA *(terme spécifique à SAP R/3)*
Interface utilisateur SAP R/3 intégrant les outils BRBACKUP, BRARCHIVE et BRRESTORE.

sauvegarde avec temps d'indisponibilité nul (ZDB)
Approche de sauvegarde selon laquelle les techniques de duplication des données fournies par une baie de disques permettent de réduire l'impact des opérations de sauvegarde sur un système d'application. Une réplique des données à sauvegarder est d'abord créée. Toutes les opérations de sauvegarde suivantes sont effectuées au niveau des données répliquées plutôt que les données d'origine, le système d'application pouvant retourner en mode de fonctionnement normal.
Voir aussi **sauvegarde avec temps d'indisponibilité nul (ZDB)**, **sauvegarde sur bande ZDB**, **ZDB sur disque + bande** et **restauration instantanée**.

sauvegarde complète
Sauvegarde au cours de laquelle tous les objets sélectionnés sont sauvegardés, qu'ils aient été ou non modifiés récemment.
Voir aussi **types de sauvegarde**.

sauvegarde de base de données complète
Sauvegarde de toutes les données d'une base de données, et non uniquement des données ayant été modifiées après la dernière sauvegarde (complète ou incrémentale) de la base de données. Une sauvegarde de base de données complète ne dépend d'aucune autre sauvegarde.

sauvegarde de base de données différentielle
Sauvegarde de base de données au cours de laquelle seules les modifications intervenues après la dernière sauvegarde complète de la base sont sauvegardées.

sauvegarde de boîte au lettres complète
Sauvegarde de tout le contenu d'une boîte aux lettres.

sauvegarde de client
Sauvegarde de tous les systèmes de fichiers montés sur un client. Les systèmes de fichiers montés sur le client une fois la spécification de sauvegarde créée ne sont pas détectés automatiquement.

sauvegarde de client avec découverte de disque
Sauvegarde de tous les systèmes de fichiers montés sur un client. Lorsque la sauvegarde commence, Data Protector découvre les disques se trouvant sur les clients. La sauvegarde du client avec découverte du disque permet de simplifier la configuration de la sauvegarde et d'améliorer la couverture de sauvegarde des systèmes sur lesquels des disques sont fréquemment montés/ démontés.

sauvegarde de CONFIGURATION Windows
Data Protector permet de sauvegarder la CONFIGURATION Windows, y compris le registre Windows, les profils utilisateur, les journaux d'événements et les données des serveurs WINS et DHCP (s'ils sont configurés) en une seule étape.

sauvegarde de disque en plusieurs étapes.
Le processus de sauvegarde des données en plusieurs étapes permet d'améliorer les performances des sauvegardes et des restaurations, de réduire les coûts de stockage des données sauvegardées et d'améliorer la disponibilité et l'accessibilité des données pour restauration. Les étapes de sauvegarde consistent à sauvegarder d'abord les données sur un type de support (par exemple un disque) puis ultérieurement les copier sur un type de support différent (par example sur bande).

sauvegarde delta
Sauvegarde contenant toutes les modifications apportées à la base de données par rapport à la dernière sauvegarde effectuée, quel que soit le type de celle-ci.
Voir aussi **types de sauvegarde**

sauvegarde de snapshot *(terme spécifique à HP StorageWorks VA et HP StorageWorks EVA)*
Voir **sauvegarde sur bande ZDB**, **sauvegarde sur disque ZDB** et **ZDB sur disque + bande**.

sauvegarde de transaction
Les sauvegardes de transaction consomment généralement moins de ressources que les sauvegardes de base de données ; elles peuvent donc être effectuées plus souvent que les sauvegardes de base de données. En effectuant des sauvegardes de transaction, l'utilisateur peut récupérer

la base de données telle qu'elle était à un moment précis précédant la survenue d'un problème.

sauvegarde de transaction *(terme spécifique à Sybase et SQL*)
Sauvegarde du journal de transactions contenant un enregistrement des modifications effectuées depuis la dernière sauvegarde complète ou la dernière sauvegarde de transaction.

sauvegarde d'hôte
Voir **sauvegarde de client avec découverte de disque**.

sauvegarde différentielle
Sauvegarde incrémentale (incr) basée sur une sauvegarde Data Protector antérieure (complète ou incrémentale) et devant être protégée.
Voir **sauvegarde incrémentale**.

sauvegarde différentielle *(terme spécifique à MS SQL)*
Sauvegarde de base de données au cours de laquelle seules les modifications intervenues après la dernière sauvegarde complète de la base sont sauvegardées.
Voir aussi **types de sauvegarde**.

sauvegarde d'image disque (rawdisk)
Sauvegarde ultra-rapide au cours de laquelle Data Protector sauvegarde les fichiers en tant qu'images bitmap. Ce type de sauvegarde (rawdisk) ne suit pas la structure des fichiers et des répertoires stockés sur le disque ; elle stocke néanmoins la structure de l'image disque au niveau des octets. Vous pouvez effectuer une sauvegarde d'image disque de certaines sections du disque ou de sa totalité.

sauvegarde directe
Solution de sauvegarde SAN au sein de laquelle la transmission directe des données entre le disque et la bande (ou un autre périphérique de stockage secondaire) est facilitée par la commande SCSI Extended Copy (Xcopy). La sauvegarde directe permet de réduire le nombre d'E/S sur les systèmes dans un environnement SAN. La commande SCSI Extended Copy (XCopy) facilite la transmission directe des données entre le disque et la bande (ou un autre périphérique de stockage secondaire). Cette commande est fournie par un élément de l'infrastucture comprenant les ponts, les commutateurs, les bibliothèques de bandes et les sous-systèmes de disques.
Voir aussi **moteur XCopy**.

sauvegarde du journal des transactions
Les sauvegardes du journal des transactions consomment généralement moins de ressources que les sauvegardes de base de données ; elles peuvent donc être effectuées plus souvent que les sauvegardes de base de données. En effectuant des sauvegardes des journaux

de transactions, l'utilisateur peut récupérer la base de données telle qu'elle était à un moment précis.

sauvegarde en ligne
Une sauvegarde effectuée alors que la base de données est accessible. La base de données passe en mode de sauvegarde spécial pendant que l'application de sauvegarde a besoin d'accéder aux données d'origine. Pendant ce laps de temps, la base de donnée est entièrement opérationnelle ; toutefois ses performances peuvent être légèrement réduites et la taille des fichiers journaux peut augmenter très rapidement.

- Pour les méthodes de sauvegarde simples (non ZDB), le mode de sauvegarde est requis pendant toute la durée de la sauvegarde (~minutes/heures). Par exemple, pour les sauvegardes sur bande, jusqu'à ce que le flux de données vers la bande soit terminé.

- Pour les méthodes ZDB, le mode de sauvegarde est requis uniquement pendant le processus de duplication des données (~secondes). Le fonctionnement normal de la base de données peut alors être rétabli pour le reste du processus de sauvegarde.

Dans certains cas, les journaux de transactions doivent également être sauvegardés pour permettre la restauration d'une base de données cohérente.
Voir aussi **sauvegarde avec temps d'indisponibilité nul (ZDB)** et **sauvegarde hors ligne**.

sauvegarde hors ligne
Une sauvegarde pendant laquelle une base de données d'application ne peut pas être utilisée par l'application.

- Pour les méthodes de sauvegarde simples (non ZDB), la base de données est généralement mise en veille, afin de permettre une utilisation par le système de sauvegarde et non par l'application, pendant toute la période de sauvegarde (~minutes/heures). Par exemple, pour les sauvegardes sur bande, jusqu'à ce que le flux de données vers la bande soit terminé.

- Pour les méthodes ZDB, la base de données est également mise en veille, mais uniquement pendant le processus de duplication des données (~secondes). Le fonctionnement normal de la base de données peut alors être rétabli pour le reste du processus de sauvegarde.

Voir aussi **sauvegarde avec temps d'indisponibilité nul (ZDB)** et **sauvegarde en ligne**.

sauvegarde incrémentale
Procédé consistant à ne sauvegarder que les fichiers auxquels des modifications ont été apportées depuis la dernière sauvegarde. L'utilisateur peut choisir parmi différents niveaux de sauvegarde incrémentale, ce qui lui permet de sélectionner uniquement les fichiers qui ont été modifiés depuis la dernière sauvegarde incrémentale.
Voir aussi **types de sauvegarde**.

sauvegarde incrémentale *(terme spécifique à Microsoft Exchange Server)*
Sauvegarde de données Microsoft Exchange Server modifiées depuis la dernière sauvegarde complète ou incrémentale. Avec la sauvegarde incrémentale, seuls les fichiers de journal des transactions sont sauvegardés.
Voir aussi **types de sauvegarde**.

sauvegarde incrémentale de boîte aux lettres
Sauvegarde toutes les modifications apportées à la boîte aux lettres depuis la dernière sauvegarde, quel que soit son type.

sauvegarde incrémentale de boîte aux lettres "incremental1"
sauvegarde toutes les modifications apportées à la boîte aux lettres depuis la dernière sauvegarde complète.

sauvegarde rawdisk
Voir **sauvegarde d'image disque**.

sauvegarde sans bande *(terme spécifique à ZBD)*
Voir **sauvegarde sur disque ZDB**.

sauvegarde Split Mirror *(terme spécifique à EMC Symmetrix)*
Voir **sauvegarde sur bande ZDB**.

sauvegarde Split Mirror *(terme spécifique à HP StorageWorks Disk Array XP)*
Voir **sauvegarde sur bande ZDB**, **sauvegarde sur disque ZDB** et **ZDB sur disque + bande**.

sauvegarde sur bande ZDB *(terme spécifique à ZBD)*
Type de sauvegarde avec temps d'indisponibilité nul caractérisé par le fait que la réplique créée est copiée en continu sur un support de sauvegarde, généralement une bande. Il est impossible d'effectuer une restauration instantanée à partir de ce type de sauvegarde. La réplique doit donc être conservée sur la baie de disques après la sauvegarde. Les données sauvegardées peuvent être restaurées à l'aide de la

restauration Data Protector standard à partir d'une bande. Sur les baies split mirror, la restauration split mirror peut également être utilisée.
Voir aussi **sauvegarde avec temps d'indisponibilité nul (ZDB)**, **sauvegarde sur disque ZDB**, **restauration instantanée**, **ZDB sur disque + bande** et **réplique**.

sauvegarde sur disque ZDB *(terme spécifique à ZBD)*
Type de sauvegarde avec temps d'indisponibilité nul caractérisé par le fait que la réplique créée est conservée sur la baie de disques en tant que sauvegarde des volumes source à un instant donné. Plusieurs répliques, créées à différents moments à l'aide de la même spécification de sauvegarde, peuvent être conservées dans un jeu de répliques. Une réplique effectuée à partir d'une sauvegarde sur disque ZDB peut être restaurée via le processus de restauration instantanée.
Voir aussi **sauvegarde avec temps d'indisponibilité nul (ZDB)**, **sauvegarde sur bande ZDB**, **ZDB sur disque + bande**, **restauration instantanée** et **rotation du jeu de répliques**.

sauvegarde système sur bande *(terme spécifique à Oracle)*
Interface Oracle chargée d'exécuter les actions nécessaires au chargement, à l'étiquetage et au déchargement des bons périphériques de sauvegarde lorsqu'Oracle émet des demandes de sauvegarde ou de restauration.

script CMD pour serveur en ligne *(terme spécifique à Informix)*
Script CMD Windows créé dans INFORMIXDIR lorsque le serveur en ligne Informix est configuré. Le script CMD est un ensemble de commandes système chargé d'exporter les variables d'environnement pour le serveur en ligne.

script shell log_full *(terme spécifique à Informix UNIX)*
Script fourni par ON-Bar et que l'utilisateur peut utiliser pour lancer la sauvegarde des fichiers journaux logiques lorsque le serveur en ligne émet une alarme de saturation de journal. Le paramètre de configuration ALARMPROGRAM Informix sélectionné par défaut est <*INFORMIXDIR*>/etc/log_full.sh, où <*INFORMIXDIR*> est le répertoire de base du serveur en ligne. Si vous ne souhaitez pas que les journaux logiques soient sauvegardés en continu, attribuez la valeur <*INFORMIXDIR*>/etc/no_log.sh au paramètre de configuration ALARMPROGRAM.

sécurité intégrée *(terme spécifique à MS SQL)*
La sécurité intégrée permet à Microsoft SQL Server d'utiliser les mécanismes

d'authentification Windows pour valider les noms de connexion de Microsoft SQL Server pour toutes les connexions. Pour l'utiliser, les utilisateurs doivent posséder un mot de passe pour Windows et pour Microsoft SQL Server. La sécurité intégrée doit être utilisée dans des environnements où tous les clients peuvent prendre en charge des "connexions approuvées". On appelle "connexions approuvées" des connexions validées par Windows Server et acceptées par Microsoft SQL Server. Seules les connexions approuvées sont autorisées.

sécurité standard *(terme spécifique à MS SQL)*
La sécurité standard utilise le processus de validation des connexions de Microsoft SQL Server pour toutes les connexions. Elle est utile dans les environnements réseau comportant une large variété de clients, dont certains peuvent ne pas prendre en charge les connexions approuvées. Elle assure également la compatibilité avec les versions antérieures de Microsoft SQL Server.
Voir aussi **sécurité intégrée**.

serveur de base de données
Ordinateur sur lequel est stockée une base de données volumineuse, telle qu'une base de données SAP R/3 ou Microsoft SQL. Une base de données stockée sur un serveur est accessible aux clients.

serveur de lecteurs multiples
Licence permettant à l'utilisateur d'exécuter un nombre illimité d'Agents de support sur un même système. Cette licence, liée à l'adresse IP du Gestionnaire de cellule, n'est plus disponible.

serveur DHCP
Système sur lequel s'exécute le protocole DHCP (Dynamic Host Configuration Protocol), permettant la configuration dynamique des adresses IP et mettant à disposition des informations connexes.

Serveur d'installation
Système informatique contenant un référentiel des packages logiciels Data Protector pour une architecture spécifique. Le Serveur d'installation permet l'installation à distance des clients Data Protector. Dans les environnements mixtes, deux Serveur d'installation au moins sont nécessaires : l'un pour les systèmes UNIX et l'autre pour les systèmes Windows.

serveur DNS
Dans le modèle client-serveur DNS, il s'agit du serveur contenant les informations relatives à une partie de la base de données DNS et rendant les

noms des ordinateurs accessibles aux programmes de résolution client en faisant une demande de résolution de noms via Internet.

serveur en ligne *(terme spécifique à Informix)*
Ce terme fait référence au serveur dynamique en ligne INFORMIX.

serveur Sybase SQL *(terme spécifique à Sybase)*
Serveur de l'architecture client-serveur Sybase. Le serveur Sybase SQL gère plusieurs bases de données et utilisateurs, assure le suivi des positions physiques des données sur les disques, établit le mappage entre la description logique des données et leur stockage physique et maintient les caches de données et de procédures en mémoire.

serveur virtuel
Machine virtuelle dans un environnement de clusters définie sur un domaine par un nom et une adresse IP réseau. Son adresse est mise en cache par le service de cluster et mappée au nœud cluster qui exécute les ressources du serveur virtuel. De cette façon, toutes les demandes concernant un serveur virtuel donné sont mises en cache par un nœud de cluster spécifique.

serveur WINS Système sur lequel s'exécute le logiciel Windows Internet Name Service chargé de la résolution des noms des ordinateurs du réseau Windows en adresses IP. Data Protector peut sauvegarder les données du serveur WINS dans le cadre de la configuration Windows.

service de réplication de fichiers (FRS)
Service Windows dupliquant les stratégies de groupe et les scripts d'ouverture de session de la banque du contrôleur de domaine. Ce service duplique également les partages de système de fichiers distribués (DFS) entre des systèmes et permet à tout serveur d'effectuer une opération de réplication.

service de réplication de sites *(terme spécifique à Microsoft Exchange Server 2000/2003)*
Service Microsoft Exchange Server 2000/2003 permettant la compatibilité avec Microsoft Exchange Server 5.5 via l'émulation du service d'annuaire Exchange Server 5.5.
Voir aussi **banque d'informations** et **service Gestionnaire de clés**.

service Microsoft Volume Shadow Copy (VSS)
Service logiciel offrant une interface de communication unifiée destinée à coordonner la sauvegarde et la restauration d'une application VSS, quelles que soient les fonctions de cette dernière. Ce service collabore avec

l'application de sauvegarde, les modules d'écriture, fournisseurs de copies miroir et le noyau du système d'exploitation pour mettre en oeuvre la gestion des copies miroir des volumes et des jeux de copies miroir.
Voir aussi **copie miroir, fournisseur de copie miroir, module d'écriture**.

service Volume Shadow Copy
Voir **service Microsoft Volume Shadow Copy**.

services Terminal Server *(terme spécifique à Windows)*
Les services Terminal Server de Windows fournissent un environnement multi-sessions permettant aux clients d'accéder à des sessions Windows virtuelles ainsi qu'à des applications Windows exécutées sur le serveur.

session de copie d'objets
Processus créant une copie supplémentaire des données sauvegardées sur un jeu de supports différent. Pendant une session de copie d'objet, les objets sauvegardés sélectionnés sont copiés à partir de la source vers le support cible.

session de gestion de supports
Session servant à exécuter une action sur un support, comme l'initialisation, l'analyse de contenu, la vérification des données stockées sur le support ou la copie du support.

session de restauration
Procédé consistant à copier les données d'un support de sauvegarde sur un système client.

session de sauvegarde
Processus consistant à créer une copie des données sur un support de stockage. Les activités sont définies dans une spécification de sauvegarde ou dans une session interactive. L'ensemble des clients configurés dans une spécification de sauvegarde est sauvegardé lors d'une session de sauvegarde unique, par le biais du même type de sauvegarde (complète ou incrémentale). Le résultat d'une session de sauvegarde est un ensemble de supports sur lesquels des données ont été écrites ; celui-ci est également appelé jeu de sauvegardes ou de supports.
Voir aussi **sauvegarde incrémentale** et **sauvegarde complète.**

session
Voir **Session de sauvegarde**, **Session de gestion de supports** et **Session de restauration**.

SGBDR
Système de gestion de base de données relationnelle.

SIBF
Les fichiers SIBF (Serverless Integrations Binary Files), ou fichiers binaires d'intégrations sans serveur,

représentent la partie de la base de données IDB stockant les métadonnées brutes NDMP. Ces données sont nécessaires à la restauration des objets NDMP.

simultanéité
Voir **agents de disque simultanés**.

SMB
Voir **sauvegarde Split Mirror**.

SMBF
La partie fichiers binaires de messages de session (SMBF) de la base de données IDB stocke les messages de session générés pendant les sessions de sauvegarde, de copie d'objet, de restauration et de gestion des supports. Chaque session génère un fichier binaire. Les fichiers sont regroupés par année et par mois.

snapshot *(terme spécifique à HP StorageWorks VA et HP StorageWorks EVA)*
Type de réplique créée à l'aide de techniques de création de snapshot. Plusieurs types de snapshot sont disponibles, présentant des caractéristiques différentes en fonction des batteries/techniques utilisées. Ces répliques sont dynamiques et peuvent être des copies virtuelles basées sur le contenu des volumes source ou des doublons exacts indépendants (clones), en fonction du type de snapshot et du temps écoulé depuis la création.
Voir aussi **réplique** et **création de snapshot**.

snapshot transportable *(terme spécifique à MS VSS)*
Copie miroir créée sur le système d'application et pouvant être présentée au système de sauvegarde effectuant la sauvegarde.
Voir aussi **Microsoft Volume Shadow Copy service (VSS)**.

spécification de sauvegarde
Liste d'objets à sauvegarder, accompagnée d'un ensemble de périphériques ou de lecteurs à utiliser, d'options de sauvegarde pour tous les objets spécifiés, ainsi que du jour et de l'heure où les sauvegardes doivent être effectuées. Les objets peuvent être des disques/volumes entiers ou une partie de ceux-ci ; il peut s'agir par exemple de fichiers, de répertoires ou du registre Windows. L'utilisateur peut définir des listes de sélection de fichiers, telles que les listes d'inclusion ou d'exclusion.

Split Mirror *(terme spécifique à EMC Symmetrix et HP StorageWorks Disk Array XP)*
Réplique créée à l'aide de techniques split mirror. Cette réplique fournit un doublon exact indépendant ou un clone du contenu des volumes source.
Voir aussi **réplique** et **création de split mirror**.

SRDF *(terme spécifique à EMC Symmetric*)
L'utilitaire SRDF (Symmetrix Remote Data Facility), ou utilitaire de gestion des données distantes Symmetrix, est un processus de continuité des activités permettant de dupliquer efficacement et en temps réel les données des SLD entre plusieurs environnements de traitement séparés. Ces environnements peuvent se trouver au sein d'un même ordinateur ou être séparés par de grandes distances.

stratégie d'allocation de supports
Procédé permettant de déterminer l'ordre d'utilisation des supports pour la sauvegarde. Dans le cas d'une stratégie d'allocation stricte, Data Protector demande un support spécifique. Dans le cas d'une stratégie souple, Data Protector demande tout support approprié. Dans le cas d'une stratégie de priorité aux supports formatés, Data Protector préfère utiliser les supports inconnus, même si des supports non protégés sont disponibles dans la bibliothèque.

stratégie d'utilisation des supports
La stratégie d'utilisation des supports permet de contrôler la manière dont les nouvelles sauvegardes sont ajoutées aux supports déjà utilisés. Ses options sont les suivantes : Ajout possible, Sans possibilité d'ajout et Ajout possible aux incrémentales uniquement.

Symmetrix Application Programming Interface (SYMAPI) *(terme spécifique à EMC Symmetrix)*
Bibliothèque de fonctions raccordable pouvant faire interface avec les systèmes EMC Symmetrix connectés aux clients Data Protector. Fourni par EMC.

système cible *(terme spécifique à la récupération après sinistre)*
Système après la survenue d'un sinistre. Le système cible est généralement non amorçable et l'objet de la récupération après sinistre consiste justement à redonner à ce système sa configuration initiale. La différence entre un système endommagé et un système cible réside dans le fait que, pour le système cible, le matériel défaillant a été remplacé.

système d'application *(terme spécifique à ZBD)*
Système sur lequel s'exécute l'application ou la base de données. Les données de l'application ou de la base de données sont situées sur les volumes source.
Voir aussi **système de sauvegarde** et **volume source**.

système de fichiers
Organisation des fichiers sur un disque dur. Un système de fichiers est enregistré pour que les attributs et le contenu des fichiers soient stockés sur le support de sauvegarde.

système de fichiers distribués (DFS)
Service reliant les partages de fichiers dans un seul espace de noms. Ces partages peuvent résider sur le même ordinateur ou sur des ordinateurs différents. Le DFS permet à un client d'accéder aux ressources de manière transparente.

système de sauvegarde *(terme spécifique à ZBD)*
Système connecté aux volumes cible d'un ou plusieurs systèmes d'applications. Le système de sauvegarde est généralement connecté à un périphérique de sauvegarde pour la copie des données sur une réplique. *Voir aussi* **système d'application**, **volume cible** et **unité de réplique**.

système d'hébergement
Client Data Protector en fonctionnement utilisé pour la récupération après sinistre avec restitution de disque à l'aide d'un Agent de disque Data Protector installé.

système d'origine
Configuration système sauvegardée par Data Protector avant qu'un sinistre ne frappe le système.

SysVol (*terme spécifique à Windows)*
Répertoire partagé contenant la copie des fichiers publics du domaine sur le serveur. Ces fichiers sont reproduits sur tous les contrôleurs du domaine.

table des journaux de transactions

(terme spécifique à Sybase)
Table système où sont enregistrées automatiquement toutes les modifications apportées à la base de données.

thread *(terme spécifique à MS SQL Server 7.0/2000)*
Entité exécutable appartenant à un seul processus. Elle comprend un compteur de programme, une pile en mode utilisateur, une pile en mode kernel et un ensemble de valeurs de registre. Plusieurs threads peuvent être exécutés en même temps dans un même processus.

TimeFinder *(terme spécifique à EMC Symmetrix)*
Processus Business Continuance permettant de créer une copie instantanée d'un ou plusieurs périphériques logiques Symmetrix (SLD). Cette copie est créée sur des SLD préconfigurés spécialement et appelés BCV ; elle est accessible via une adresse de périphérique distincte.

TLU
Tape Library Unit ou unité de bibliothèque de bandes.

TNSNAMES.ORA *(terme spécifique à Oracle et SAP R/3)*
Fichier de configuration réseau

contenant des descripteurs de connexion mappés à des noms de services. La maintenance du fichier peut s'effectuer au niveau central ou au niveau local, afin d'être accessible à tous les clients ou à chacun d'entre eux individuellement.

transaction
Mécanisme destiné à s'assurer qu'un ensemble d'actions est considéré comme une seule unité de travail. Les bases de données utilisent les transactions pour effectuer un suivi des modifications.

type de support
Type physique d'un support, comme DDS ou DLT.

types de sauvegarde
Voir **sauvegarde incrémentale**, **sauvegarde différentielle**, **sauvegarde de transaction**, **sauvegarde complète** et **sauvegarde delta**.

unité de commande principale (MCU, pour Main Control Unit) *(terme spécifique à HP StorageWorks Disk Array XP)*
Baie de disques HP StorageWorks Disk Array XP contenant les volumes principaux pour la configuration en accès continu et agissant comme périphérique maître.
Voir aussi **BC** *(terme spécifique à HP StorageWorks Disk Array XP)*, **CA** *(terme spécifique à HP StorageWorks Disk Array XP)* et **LDEV HP StorageWorks Disk Array XP**.

unité de télécommande (RCU) *(terme spécifique à HP StorageWorks Disk Array XP)*
Unité agissant comme esclave d'une MCU dans une configuration AC. Dans les configurations bidirectionnelles, la RCU peut également agir comme une MCU.

utilitaire onbar *(terme spécifique à Informix)*
Utilitaire Informix chargé de communiquer les demandes de sauvegarde et de restauration au serveur en ligne. Cet utilitaire fait appel à XBSA pour échanger des données de contrôle, de sauvegarde et de restauration avec Data Protector.

VBFS *(terme spécifique à OmniStorage)*
Un VBFS (Very Big File System), ou très gros système de fichiers, est une extension du système de fichiers HP-UX standard sur HP-UX 9.x. Il est monté sur un répertoire comme n'importe quel système de fichiers HP-UX. Dans un VBFS, seules les informations de superblock, d'inode et d'attribut étendu demeurent en permanence sur le disque dur et ne migrent jamais.
Voir aussi **MFS**.

vérification
Fonction permettant à l'utilisateur de contrôler si les données Data Protector stockées sur un support spécifique sont lisibles. En outre, si l'option CRC (cyclic redundancy check) était activée lors de la sauvegarde, l'utilisateur peut contrôler la cohérence des blocs.

version de fichier
Un même fichier peut être sauvegardé plusieurs fois lors de sauvegardes complètes et incrémentales (si des modifications ont été apportées au fichier). Si le niveau de journalisation sélectionné pour la sauvegarde est TOUT, Data Protector conserve dans la base de données IDB une entrée pour le nom de fichier lui-même et une pour chaque version (date/heure) du fichier.

Virtual Controller Software (VCS)

(terme spécifique à HP StorageWorks)
Micrologiciel gérant tous les aspects du fonctionnement du système de stockage, dont les communications avec Command View EVA via les contrôleurs HSV.
Voir aussi **Command View (CV) EVA**.

volser *(terme spécifique à ADIC et STK)*
Un volser (VOLume SERial number - numéro de série de volume) est une étiquette située sur le support et servant à identifier la bande physique dans les très grandes bibliothèques. Il s'agit d'une appellation spécifique aux périphériques ADIC/GRAU et StorageTek.

volume cible *(terme spécifique à ZBD)*
Un volume de stockage sur lequel les données sont dupliquées.

volume de stockage *(terme spécifique à ZBD)*
Un volume de stockage représente un objet pouvant être présenté à un système d'exploitation ou à une autre entité (par exemple, un système de virtualisation) sur lequel existent des systèmes de gestion de volumes, des systèmes de fichiers ou d'autres objets. Les systèmes de gestion de volumes et les systèmes de fichiers sont basés sur ce type de stockage. Habituellement, ils peuvent être créés ou existent déjà dans un système de stockage tel qu'une baie de disques.

volume/disque/partition d'amorçage
Volume/disque/partition contenant les fichiers nécessaires à la première étape du processus d'amorçage. La terminologie utilisée par Microsoft définit le volume/disque/partition d'amorçage comme le volume/disque/partition contenant les fichiers du système d'exploitation.

volume/disque/partition système
Volume/disque/partition contenant les fichiers du système d'exploitation. La

terminologie utilisée par Microsoft définit ces éléments comme ceux contenant les fichiers nécessaires pour assurer les premières étapes du processus d'amorçage.

volume principal (P-VOL) *(terme spécifique à HP StorageWorks Disk Array XP)*
Il s'agit de LDEV HP StorageWorks Disk Array XP standard agissant comme volume principal pour les configurations CA et BC. Le P-VOL est situé dans le MCU.
Voir aussi **volume secondaire (S-VOL)**.

volume secondaire (S-VOL) *(terme spécifique à HP StorageWorks Disk Array XP*)
LDEV XP agissant comme miroir CA ou BC secondaire d'un autre LDEV (P-VOL). Dans le cas d'un CA, les S-VOL peuvent être utilisés comme périphériques de secours dans une configuration MetroCluster. Des adresses SCSI distinctes, différentes des adresses utilisées par les P-VOL, sont attribuées aux S-VOL.
Voir aussi **volume principal (P-VOL).**

volume source *(terme spécifique à ZBD)*
Volume de stockage contenant les données à répliquer.

VPO
Voir **OVO**.

VSS
Voir **service Microsoft Volume Shadow Copy**.

VxFS
Veritas Journal Filesystem, système de fichiers journaux Veritas.

VxVM (Veritas Volume Manager)
Le VVM (Veritas Volume Manager), ou Gestionnaire de volume Veritas, est un système permettant de gérer l'espace disque sur les plates-formes Solaris. Un système VxVM est constitué de groupes arbitraires d'un ou plusieurs volumes physiques organisés en groupes de disques logiques.

Wake ONLAN
Fonction de mise en marche à distance pour les systèmes s'exécutant en mode d'économie d'énergie à partir d'un autre système se trouvant sur le même réseau local.

Web Reporting
Fonction Data Protector permettant à l'utilisateur d'afficher des rapports sur le statut de sauvegarde et sur la configuration Data Protector à l'aide de l'interface Web.

ZDB
Voir **sauvegarde avec temps d'indisponibilité nul (ZDB)**.

ZDB sur disque + bande *(terme spécifique à ZBD)*
Type de sauvegarde avec temps d'indisponibilité nul caractérisé par le fait que la réplique créée est conservée sur la baie de disques en tant que sauvegarde des volumes source à un instant donné, de la même manière que la sauvegarde sur disque ZDB. Toutefois, les données de la réplique peuvent également être copiées en mode continu sur un support de sauvegarde, tout comme la sauvegarde sur bande ZDB. Si cette méthode de sauvegarde est utilisée, les données sauvegardées dans la même session peuvent être restaurées via le processus de restauration instantanée, la restauration Data Protector standard à partir d'une bande, ou, sur des baies split mirror, via la restauration split mirror.
Voir aussi **sauvegarde avec temps d'indisponibilité nul (ZDB)**, **sauvegarde sur disque ZDB**, **sauvegarde sur bande ZDB**, **restauration instantanée**, **réplique** et **rotation du jeu de répliques**.

C

D

E

F

G

H

I

J

R

S

T

Index