HP Data Protector for PCs 7.0
Manuel d'installation et d'administration

Référence HP : n/a
Date de publication : Juin 2011
Édition : Première

Sommaire

Présentation du manuel

Ce manuel fournit des informations sur les éléments suivants :

- Installation de HP Data Protector for PCs
- Configuration des stratégies de HP Data Protector for PCs
- Logiciel Agent de HP Data Protector for PCs sur les ordinateurs de bureau et les ordinateurs portatifs des utilisateurs
- Définition du nombre de Agents qui peuvent être pris en charge
- Obtention de l'assistance pour Data Protector for PCs

Public cible

Ce manuel a été rédigé pour les administrateurs qui souhaitent installer et configurer HP Data Protector for PCs. Certaines connaissances dans le domaine suivant seront utiles :

- Administration Windows

Conventions et symboles utilisés dans ce document

Convention	Élément
Texte bleu : « Présentation du manuel » (page 5)	Liens de référence croisée et adresses de messagerie
Texte bleu souligné : http://www.hp.com	URL
Texte en **caractères gras**	• Touches enfoncées • Texte tapé dans un élément de l'interface utilisateur graphique tel qu'une zone • Éléments de l'interface utilisateur graphique que l'utilisateur peut sélectionner ou sur lesquels il peut cliquer comme des éléments de menu ou de liste, des boutons, des onglets et des cases.
Texte en *caractères italiques*	Texte en emphase

Convention	Élément
Texte en `police monoespace`	• Noms de fichiers et de répertoires • Résultats du système • Code • Instructions, arguments et valeur des arguments
Texte en *`police monoespace et italique`*	• Variables du code • Variables des instructions
Texte en **`police monoespace et caractères gras`**	Texte en police monoespace mis en emphase

IMPORTANT : Fournit des clarifications ou des instructions particulières.

REMARQUE : Fournit des informations complémentaires.

Informations générales

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

Assistance technique HP

Pour obtenir des informations sur l'assistance technique internationale, consultez le site Web d'assistance de HP :

http://www.hp.com/support

Avant de prendre contact avec HP, recueillez les informations suivantes :

- Noms et numéros des modèles de produit
- Numéro d'enregistrement pour l'assistance technique (le cas échéant)
- Numéros de série des produits
- Messages d'erreur
- Type de système d'exploitation et niveau de révision
- Questions détaillées

Service d'abonnement

HP vous invite à enregistrer votre produit sur le site Web de Subscriber's Choice for Business à l'adresse

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

Une fois que vous aurez enregistré le produit, vous recevrez des notifications par courrier électronique sur les améliorations des produits, les nouvelles versions de pilote, les mises à niveau de microprogramme et d'autres ressources sur les produits.

sites Web HP

Pour obtenir des informations complémentaires, consultez les sites Web HP suivants :

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

Commentaires sur la documentation

HP apprécie vos commentaires.

Si vous avez des commentaires ou des suggestions à formuler sur la documentation qui accompagne les produits, écrivez à **DP.DocFeedback@hp.com**. Tous les envois deviennent la propriété de HP.

1 Vue d'ensemble et configuration requise

Vue d'ensemble de Data Protector for PCs

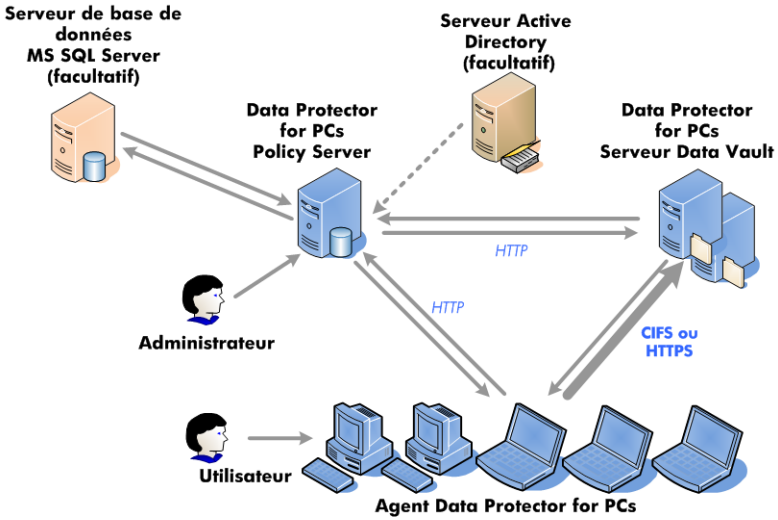
HP Data Protector for PCs réunit deux composants logiciels principaux, à savoir le Policy Server et les Agents. Le Policy Server est exécuté sur un serveur Windows. Consultez la matrice de prise en charge afin de connaître les versions prises en charge (https://h20230.www2.hp.com/selfsolve/manuals). Les Agents sont exécutés en arrière-plan sur chaque ordinateur de bureau ou portable.

Le Policy Server a également accès aux groupes et aux unités d'organisation au sein d'un serveur Active Directory.

Les données des utilisateurs sont sauvegardées dans les Data Vaults. Le serveur Data Vault doit être séparé du Policy Server. Si vous utilisez des Data Vaults de type partage de fichiers Windows au lieu des Data Vaults Web recommandés, ils se trouvent sur un ou plusieurs partages de fichiers Windows sur des serveurs de fichiers.

Le schéma suivant illustre l'architecture de Data Protector for PCs :

Figure 1 Architecture de Data Protector for PCs



Différentes stratégies définissent les fichiers sauvegardés depuis les ordinateurs de bureau et portables et l'emplacement où ces sauvegardes sont conservées. Ces stratégies sont définies via la console de Policy Serveur. Les stratégies sont ensuite distribuées automatiquement aux Agents, à l'aide du protocole SOAP sur le port HTTP 80. Les stratégies sont conservées sur le Policy Server.

Les Agents exécutent ces stratégies. Quand un utilisateur modifie un fichier de données protégé conformément aux stratégies, une version antérieure est créée sur le disque dur

local de l'ordinateur de bureau ou de l'ordinateur portable et les modifications appliquées au fichier sont compressées et copiées dans tous les Data Vaults concernés.

À chaque sauvegarde de fichier, l'Agent prévient le Policy Server qui contient un historique des audits des modifications de fichier introduites par les utilisateurs. De plus, chaque Agent envoie à intervalle régulier des informations relatives à l'intégrité au Policy Server. Vous pouvez générer des rapports sur ces données à l'aide de la console de Policy Server.

Les Data Vaults se trouvent sur le serveur Data Vault. Les données client sont copiées sur les Data Vaults via deux protocoles différents : CIFS (pour les Data Vaults de type partage de fichiers Windows) ou HTTP (pour les Data Vaults Web).

Le serveur Data Vault doit se trouver sur un autre système que le Policy Server. Pour HTTPS, le logiciel du serveur Data Vault Web est exécuté, ainsi que le logiciel Cleanup de Data Protector for PCs. Pour les Data Vaults de type partage de fichiers Windows, seul le logiciel Cleanup est installé.

Si vous utilisez Active Directory, vous pouvez configurer le Policy Server pour qu'il puisse accéder à vos groupes et unités d'organisation. Vous pouvez ensuite affecter des Data Vaults aux utilisateurs en fonction du groupe ou de l'unité d'organisation auxquels ils appartiennent. Vous pouvez également choisir les utilisateurs dans les rapports en fonction de leur appartenance.

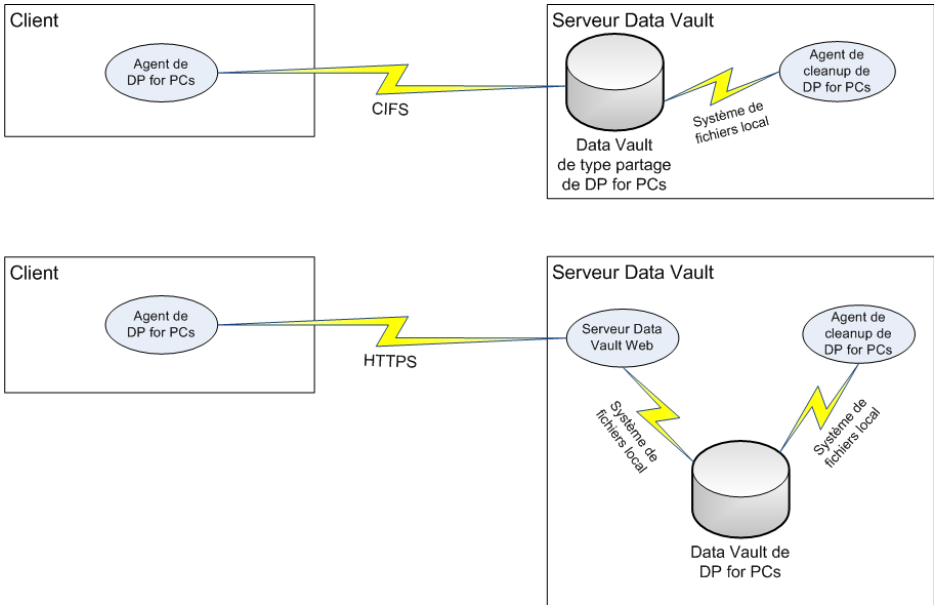
Data Vaults

Deux types de Data Vaults sont disponibles dans Data Protector for PCs :

- Data Vaults Web : basés sur le protocole HTTPS. Ils offrent le meilleur niveau de sécurité et un meilleur rendement dans les environnements à forte latence et par conséquent, ce sont eux qui sont recommandés.
- Data Vaults de type partage de fichiers Windows : basés sur le protocole CIFS, utilisés dans les versions plus anciennes de Data Protector for PCs.

La structure de données des deux types de Data Vault est identique, si bien que vous pouvez convertir les Data Vaults de type partage de fichiers Windows existants en Data Vault Web.

Figure 2 Comparaison des Data Vaults de type partage de fichiers Windows et des Data Vaults Web



Gestion des certificats

L'utilisation du protocole SSL est obligatoire pour les Data Vaults Web. Le type de certificat est défini lors de l'installation du Data Vault Web. Afin d'offrir un produit qui puisse fonctionner directement, par exemple pour une évaluation, vous pouvez installer le serveur Data Vault Web avec un certificat auto-signé. Ce type de certificat n'est pas aussi sûr qu'un certificat émis par une autorité de confiance. Pour garantir une sécurité complète, il faut importer pour le serveur Data Vault un certificat signé par une autorité de confiance dans votre environnement et l'ajouter au composant serveur.

Certificats auto-signés

Lors de la création d'une stratégie de Data Vault, vous pouvez indiquer si les certificats auto-signés sont autorisés. Aucune action n'est requise sur l'agent dans ce cas. La validité d'un certificat auto-signé émis par l'installation est limitée à 20 ans.

Certificats importés

La procédure d'importation attend un seul fichier au format PEM contenant à la fois la clé secrète et le certificat correspondant comprenant la clé publique. Il faut savoir que le fichier est copié tel quel dans le répertoire de configuration du serveur Data Vault Web. Il se peut qu'il soit chiffré, en fonction de la procédure utilisée pour créer le fichier de certificat. Dans ce cas, le processus du service Windows qui exécute le serveur Data Vault Web affichera une invite interactive pour obtenir le mot de passe de déchiffrement. Cela se produira pendant l'installation et également à chaque redémarrage du service,

par exemple après un redémarrage du système. Bien qu'il soit possible d'ajouter ce mot de passe manuellement au fichier de configuration du serveur Web pour éviter l'invite, cette action n'est pas prise en charge par le processus d'installation. Il est déconseillé d'avoir un fichier de certificat chiffré et de stocker le mot de passe dans un autre fichier juste à côté.

REMARQUE :
L'expression « autorité de confiance » implique que les ordinateurs client qui exécutent les agents considèrent cette autorité de certification comme une autorité fiable et acceptent les certificats qu'elles signent. On suppose que les magasins de certificats Windows des ordinateurs client ont déjà été configurés comme il le fallait en ajoutant le certificat de l'autorité de certification et d'autres certificats dans leurs chaînes. L'agent ne possède aucun mécanisme pour établir cette confiance. Il s'appuie sur les mécanismes de Windows.

Échange du certificat

Il est possible d'échanger le certificat sur le serveur Data Vault Web à n'importe quel moment après l'installation à l'aide de l'utilitaire `DvConfig` décrit dans le paragraphe consacré à l'interface de ligne de commande « Configuration des options de Data Vaults Web à l'aide de l'interface de ligne de commande (DvConfig) » (page 21). Ainsi, vous pouvez configurer à nouveau une installation configurée au début à l'aide d'un certificat auto-signé afin qu'elle utilise un certificat importé.

Vue d'ensemble de l'installation de Data Protector for PCs

REMARQUE : Si vous réalisez une mise à jour d'une installation de Data Protector for PCs, reportez-vous au « Mise à jour de Data Protector for PCs » (page 41).

L'installation de Data Protector for PCs comporte trois étapes :

1. **Installation du Policy Server de Data Protector for PCs.**

   Voir le « Installation du Policy Server de Data Protector for PCs » (page 14).

2. **Installation du logiciel du serveur Data Vault Web de Data Protector for PCs.**

   Voir le « Installation, configuration et maintenance du serveur Data Vault Web » (page 18).

3. **Configuration des stratégies de protection.**

   Voir le « Configuration des stratégies de protection de Data Protector for PCs » (page 23).

4. **Installation des Agents de Data Protector for PCs sur les ordinateurs portables et les ordinateurs de bureau**.

   Voir le « Installation d'agents Data Protector for PCs » (page 37).

Configuration requise

Policy Server

Pour connaître les systèmes d'exploitation pris en charge, consultez la matrice de prise en charge.

REMARQUE : *Installation sur le système d'exploitation Windows 2003 64 bits :* Policy Server tourne en mode comptabilité 32 bits sur un système d'exploitation Windows 64 bits. Cela signifie que Internet Information Services (IIS) doit être exécuté en mode 32 bits. Si ce n'est pas le cas, l'installation le remarquera lors de la vérification de la configuration requise. Vous aurez alors la possibilité de placer IIS en mode 32 bits. Si d'autres applications Web du serveur requièrent le fonctionnement d'IIS en mode 64 bits (par exemple Microsoft Exchange 2007 avec messagerie Internet, Outlook Web Access), vous serez dans l'impossibilité d'installer le Policy Server sur ce serveur. Ceci ne concerne pas l'installation d'un Policy Serveur sous Windows 2008.

Les éléments suivants doivent être installés sur le serveur :

- Internet Information Services 6.0, 7.0, 7.5 ou suivant avec prise en charge des applications ASP.NET.

  Pour Windows 2003, IIS 6.0 est une configuration requise et doit être installé avant que le Policy Server ne puisse être installé. Pour Windows 2008, Data Protector for PCs propose l'installation d'IIS 7.0 et 7.5 au cas où ils ne seraient pas installés.

- Microsoft ASP.NET 2.0

Les éléments suivants doivent également être installés sur le serveur.

- Microsoft Installer 3.1 ou suivant (requis pour .NET Framework 2.0 SP1).
- Microsoft .NET Framework 2.0 SP1 ou suivant. L'Assistant installera la version 2.0 SP1.
- Microsoft SQL Express (si aucune autre version SQL n'est présente)

De même, pour Internet Information Services 7.0 et 7.5 uniquement, les composants IIS suivants sont requis. Au cas où ils ne seraient pas installés, l'Assistant vous offre la possibilité de remédier à cette lacune :

- Serveur Web de contenu statique IIS : requis pour le service des fichiers html statiques, des documents et des images.
- IIS ASP.NET : requis pour le déploiement d'ASP.NET 2.0 et de .NET Framework
- Sécurité IIS : requise pour utiliser l'authentification Windows intégrée utilisée pour la console de Policy Server.
- IIS 6 Management Compatibility : pour permettre à l'installation de configurer IIS 6 et IIS 7 de la même manière le plus loin possible

Base de données

Data Protector for PCs doit avoir accès à une base de données Microsoft SQL Server. Consultez la matrice de prise en charge pour connaître les versions prises en charge.

Vous pouvez vérifier (et modifier) le mode d'authentification de votre installation de SQL Server à l'aide de Microsoft Enterprise Manager :

1. Cliquez avec le bouton droit de la souris sur l'instance de SQL Server, choisissez **Propriétés**, puis cliquez sur l'onglet **Sécurité**.
2. L'option **SQL Server et Windows** (au lieu de l'option **Windows seulement**) devrait déjà être sélectionnée. Si ce n'est pas le cas, sélectionnez-la, puis cliquez sur **OK**.

Vous pouvez également installer une instance de SQL Server Express Edition de Microsoft pendant l'installation de Data Protector for PCs.

Serveur Data Vault Web Data Protector for PCs

- Le serveur Data Vault Web doit être installé sur un autre système que le Policy Server. (L'installation sur le même système est possible, mais cette option convient uniquement à des fins d'évaluation).
- La version 1.6 ou suivante de l'environnement d'exécution Java doit être installée.
- Les variables `JAVA_HOME` et `JRE_HOME` doivent indiquer le répertoire d'installation de Java Runtime.

Agents Data Protector for PCs

Le logiciel Agent Data Protector for PCs peut être installé sur les ordinateurs de bureau et les ordinateurs portatifs d'utilisateur sous Windows. Pour connaître les plateformes prises en charge, consultez la matrice de prise en charge.

2 Installation du Policy Server de Data Protector for PCs

REMARQUE : Vous pouvez mettre à jour une installation existante de Policy Server de Data Protector for PCs en suivant la procédure d'installation standard. Voir la section « Mise à jour du Policy Server » (page 41) pour les détails.

Installation rapide

Voir la section « Policy Server » (page 12) pour connaître la configuration requise pour le Policy Server de Data Protector for PCs.

1. Insérez le CD-ROM d'installation de Data Protector for PCs. Si l'Assistant d'installation ne démarre pas automatiquement, exécutez-le manuellement en double-cliquant sur `setup.hta` à la racine du CD-ROM d'installation.
2. Suivez les instructions affichées à l'écran.
3. Le Policy Server Data Protector for PCs doit avoir accès à une base de données Microsoft SQL Server. Sélectionnez l'option **Utiliser l'instance Data Protector for PCs existante de Microsoft SQL Server Express** ou cliquez sur **Utiliser une instance existante de Microsoft SQL Server** . Si vous décidez d'utiliser un serveur SQL existant, vous devez fournir la chaîne de connexion au serveur de la base de données ainsi que les informations d'identification d'un compte possédant des privilèges suffisants pour créer une base de données.
4. Cliquez sur **Installer** dans la page **Installer Policy Server de Data Protector for PCs** de l'Assistant pour lancer l'installation.
5. Une fois l'installation terminée, cliquez sur **Suivant**. Vous pouvez décider ensuite d'exécuter la console de Policy Server de Data Protector for PCs.
6. Installez le serveur Data Vault Web sur un système distinct. Cliquez sur **Installer Data Vault** sur l'écran d'installation principal.

REMARQUE : Lors de l'installation, le logiciel Cleanup est toujours installé avec le logiciel du serveur Data Vault Web. Pour un serveur Data Vault qui abrite uniquement des Data Vaults de type partage de fichiers Windows, il est conseillé de l'installer localement sur un Data Vault afin d'optimiser les performances.

Installation détaillée

REMARQUE :
Serveur Windows 2003 uniquement : vous pouvez uniquement installer le Policy Server Data Protector for PCs depuis un CD-ROM partagé sur le réseau ou depuis un partage de fichiers de réseau si la stratégie de sécurité du runtime de .NET 2.0 Framework pour ce serveur est configurée sur *Confiance totale* pour la zone de sécurité Intranet local. Si votre serveur n'est pas équipé d'un lecteur de CD-ROM local, changez la stratégie de sécurité du runtime pour la zone de sécurité Intranet local sur *Confiance totale* à l'aide de l'outil de configuration de .NET Framework 2.0 dans les outils d'administration ou copiez le dossier Server depuis le CD vers un disque local sur le serveur.

Vous devez être connecté sous un compte « administrateur » pour pouvoir installer le Policy Server de Data Protector for PCs.

1. Insérez le CD-ROM d'installation de Data Protector for PCs. Si l'Assistant d'installation ne démarre pas automatiquement, exécutez-le manuellement en double-cliquant sur `setup.hta` à la racine du CD-ROM d'installation.
2. Cliquez sur **Installer le Policy Server**.

   Si l'Assistant le propose, choisissez l'option **Ouvrir** (ou **Exécuter**) ce programme depuis son emplacement actuel au lieu de **Enregistrer ce programme sur le disque**.
3. Le Policy Server de Data Protector for PCs requiert .NET Framework 2.0 SP1. S'il n'est pas encore installé, vous êtes invité à l'installer depuis le CD-ROM.

   L'installation requiert Windows Installer 3.1 ou suivant. Si nécessaire, vous aurez la possibilité d'installer Windows Installer 3.1 depuis le CD.
4. L'Assistant d'installation vérifie que la configuration requise est respectée :
   - Internet Information Services (IIS)
   - ASP.NET 2.0

   Si l'un des deux manque, cliquez sur l'élément dans la liste pour savoir comment l'installer.

   Cliquez sur **Suivant**.
5. Installez le serveur Microsoft SQL.

   Pour utiliser une instance existante de Microsoft SQL Server

   a. Cliquez sur **Utiliser une instance existante de Microsoft SQL Server**.

b. Saisissez, dans le champ **Serveur de base de données**, la chaîne de connexion au serveur de base de données existant.

c. Dans les champs **Connexion** et **Mot de passe**, saisissez les informations d'identification d'un compte possédant les privilèges suffisants pour créer une base de données. En général, il s'agira du compte « sa ».

d. Cliquez sur **Suivant**. Les informations de connexion saisies permettront de réaliser un essai de connexion au serveur de base de données existant. Si la connexion s'établit, l'Assistant passe à l'étape 6.

Pour installer l'instance Data Protector for PCs de Microsoft SQL Server Express Edition

a. Choisissez l'option **Installer une instance de DataProtectorNE Microsoft SQL Server Express**, puis cliquez sur **Suivant**.

b. Cliquez sur **Installer** afin d'installer une instance de Microsoft SQL Server 2005 Express Edition appelée « DataProtectorNE ». Cliquez sur **Suivant** une fois l'installation terminée.

6. Installez le du logiciel Policy Server de Data Protector for PCs.

   a. Sur l'écran d'accueil, cliquez sur **Suivant** pour lancer l'installation.

   - La console de Policy Server de Data Protector for PCs sera installée en tant qu'application Web dans le répertoire virtuel `C:\Inetpub\wwwroot\dpnepolicy`.
   - Le service Web Data Protector for PCs sera installé dans `C:\Inetpub\wwwroot\dpnepolicyservice`.

   Ils utilisent tous deux le protocole HTTP sur le port 80.

   b. Cliquez sur **Fermer**, puis sur **Suivant** à la fin de l'installation de Policy Server.

7. Il faut maintenant installer le programme Cleanup. Cliquez sur **Installer** pour lancer l'installation.

8. Une fois l'installation de cleanup terminée, cliquez sur **Suivant**.

   Vous administrez Data Protector for PCs de manière centralisée depuis la console de Policy Server de Data Protector for PCs. Vu que la console est accessible à l'aide d'un navigateur, vous pouvez gérer Data Protector for PCs depuis n'importe quel ordinateur qui peut établir une connexion par navigateur au Policy Server (via le port HTTP 80).

   Pour exécuter la console de Policy Server de Data Protector for PCs depuis un navigateur sur le Policy Server, laissez la case **Exécuter la console du Policy Server** cochée et cliquez sur **Terminer**.

REMARQUE : Lors de l'installation, le logiciel Cleanup est installé sur le Policy Server. Il est conseillé de l'installer également sur les Data Vaults afin d'optimiser les performances.

REMARQUE :

Paramètres du navigateur pour la console de Policy Server : si vous ne parvenez pas à afficher les pages de la console de Policy Server dans votre navigateur, vérifiez les paramètres de sécurité de celui-ci. La console requiert les éléments suivants :

- JavaScript doit être activé.
- Le bloqueur de popups doit être désactivé pour le site Web dpnepolicy.
- Il se peut que d'autres paramètres de sécurité doivent être modifiés en fonction de votre navigateur et de sa version.

Installation avec Microsoft SharePoint : quand le Policy Server est installé sur un serveur qui exécute Microsoft SharePoint, il se peut que vous receviez l'erreur 404 "Page introuvable" quand vous exécutez la console de Policy Server. L'article http://support.microsoft.com/kb/828810 de la base de connaissances de Microsoft décrit le problème et fournit la solution. Sachez que ce problème touche toutes les applications Web ASP .NET et pas seulement le Policy Server.

Pour que le Policy Server puisse être exécuté sur un serveur qui utilise SharePoint, vous devez réaliser les opérations suivantes :

1. Utiliser les outils d'administration SharePoint afin de créer des exclusions pour les deux applications Web Policy Server : `dpnepolicy` et `dpnepolicyservice`.
2. Modifier les deux fichiers `web.config` du Policy Server (`dpnepolicy\web.config` et `dpnepolicyservice\web.config`) afin d'ajouter le code XML `<httpHandlers>` et `<trust>` comme indiqué dans l'article de la base de connaissances Microsoft cité ci-dessus.

3 Installation, configuration et maintenance du serveur Data Vault Web

Installation et configuration du serveur Data Vault Web

REMARQUE : Installez le serveur Data Vault Web sur un autre système que le Policy Server. (L'installation sur le même système est possible, mais cette option convient uniquement à des fins d'évaluation).

1. Insérez le CD-ROM d'installation de Data Protector for PCs. Si l'Assistant d'installation ne démarre pas automatiquement, exécutez-le manuellement en double-cliquant sur `setup.hta` à la racine du CD-ROM d'installation.
2. Cliquez sur **Installer Data Vault**.
3. Choisissez entre :
   - **Serveur Data Vault Web** (recommandé). Le logiciel Cleanup est alors installé également sur le serveur.
   - **Logiciel Cleanup pour Data Vault de type partage de fichiers Windows**. Choisissez cette option si vous avez l'intention d'utiliser uniquement des Data Vaults de type partage de fichiers Windows.

   Voir la section « Data Vaults » (page 9) pour plus d'informations.
4. Suivez les instructions à l'écran pour terminer l'installation.
5. Après avoir obtenu une licence du Policy Server, si vous installez un serveur Web Data Vault, il faut configurer le Data Vault Web.

   Sur l'écran des paramètres du serveur, saisissez le nom de domaine complet (FQDN) et le port SSL du serveur. Il faudra utiliser le même FQDN au moment de la configuration de la stratégie de Data Vault Web sur le Policy Server. Tous les systèmes client doivent pouvoir résoudre le nom, sans quoi il sera impossible de réaliser la sauvegarde de certains d'entre eux sur les Data Vaults de ce système.
6. Sur l'écran des paramètres du certificat, vous devez choisir entre les options suivantes :
   - Importation d'un certificat SSL existant émis par une autorité de confiance(autorité de certification). Il s'agit de l'option recommandée qui offre le niveau de sécurité le plus élevé.
   - Création d'un certificat SSL auto-signé. Cette option fournit un niveau de sécurité inférieur et doit être utilisée uniquement dans le cadre d'évaluation.

REMARQUE : Il est possible d'échanger le certificat sur le serveur Data Vault Web à n'importe quel moment après l'installation à l'aide de l'utilitaire `DvConfig`. Ceci implique la reconfiguration d'une installation dotée d'un certificat auto-signé afin qu'elle utilise un certificat importé. Voir la section « Configuration des options de Data Vaults Web à l'aide de l'interface de ligne de commande (DvConfig) » (page 21).

7. L'écran suivant propose d'indiquer deux noms pour deux types d'utilisateur du serveur Data Vault Web :
   - **Utilisateur administratif**, qui s'occupe des tâches d'administration telles que la création et la suppression de Data Vaults et la migration des données de sauvegarde client.
   - **Utilisateur de la sauvegarde**, qui exécute des opérations d'utilisateur final telles que la sauvegarde ou la restauration de fichiers.

   Ces utilisateurs sont propres au serveur Data Vault Web Data Protector for PCs. Il faudra saisir les détails relatifs aux deux types lors de la création ou de la modification de Data Vaults Web pour ce serveur.

   REMARQUE : Les mots de passe doivent contenir au moins 8 caractères.

8. Cliquez sur **Suivant**, puis sur **Terminer** pour terminer l'installation et la configuration du serveur Data Vault Web et l'installation du logiciel Cleanup.

Maintenance de Data Vaults Web

1. Sur la page Stratégie de Data Vault, saisissez le nom de domaine complet du serveur et le port SSL, ainsi que les informations d'identification du compte Utilisateur de la sauvegarde. Cliquez ensuite sur **Configurer le Data Vault**.
2. Envoyez les informations d'identification de l'utilisateur administratif et la page Maintenir la page du serveur Data Vault Web s'affiche.

   Cette page permet de sélectionner ou de supprimer des Data Vaults Web. Vous pouvez également ajouter un nouveau Data Vault.

   REMARQUE : Vous pouvez uniquement sélectionner un Data Vault existant qui n'est pas connecté actuellement à une autre stratégie de Data Vault.

3. Veillez à enregistrer la stratégie de Data Vault en cliquant sur **Enregistrer** en bas de la page.
4. Si vous avez ajouté un nouveau Data Vault, vous avez la possibilité de tester l'existence et la configuration adéquate du vault.

Migration de données depuis un Data Vault de type partage de fichiers Windows existant vers un Data Vault Web

L'organisation des données dans un Data Vault demeure identique pour les Data Vaults de type partage de fichiers Windows et de type Web. Cela signifie que vous pouvez migrer les données depuis des Data Vaults existants de DPNE 6.x vers de nouveaux Data Vaults Web.

REMARQUE : La migration de données peut être réalisée uniquement pour les Data Vaults qui appartiennent au même Policy Server ou qui partagent le même mot de passe du chiffrement.

Deux scénarios existent pour la migration de données :

- Utilisation du même système pour héberger le Data Vault Web.

  REMARQUE : L'accès au même répertoire en parallèle via un partage de fichier Windows et un Data Vault Web n'est pas pris en charge.

- Déplacement de tout le Data Vault vers un autre système.

Dans les deux cas, le serveur Data Vault Web doit être installé localement sur le système où les données vont se trouver.

Pour migrer les données depuis un Data Vault de type partage de fichiers Windows existant vers un Data Vault Web

REMARQUE :

- Réalisez la migration en dehors des heures de bureau pour minimiser l'impact de l'exécution des sauvegardes.
- Ouvrez le Gestionnaire de tâches Windows pour confirmer que `DPNECleanup.exe` n'est pas en cours d'exécution.
- Vérifiez la stratégie de cleanup sur le Policy Server pour confirmer que l'exécution de `DPNECLeanup.exe` n'est pas prévue pendant la période de migration.

1. Installez le serveur Data Vault Web et mettez le Policy Server et les agents à jour à la version 7.0. Veillez à ce que tous les agents aient été redémarrés après l'installation de la version 7.0 car ce n'est qu'à cette condition qu'ils pourront commencer à sauvegarder les données sur le Data Vault Web.
2. Désactivez la stratégie de partage de fichiers Windows adéquate sur la page de la stratégie de Data Vault afin que les agents arrêtent de copier les données dans le Data Vault.
3. Si vous avez l'intention d'utiliser le même répertoire pour le Data Vault Web, arrêtez de partager le répertoire via CIFS.
4. Si le serveur Data Vault Web se trouve sur un serveur différent de celui du Data Vault de type partage de fichiers Windows, les données doivent être copiées sur

cet ordinateur dans un dossier dont le chemin ne compte pas plus de 67 caractères. Si le Data Vault se trouve sur le même serveur, il n'est pas nécessaire de copier les données vers le nouvel emplacement, sauf si vous le souhaitez pour d'autres raisons.

5. Avant de créer le Data Vault Web, définissez le comportement du processus de mise à jour initiale. Vous pouvez passer la mise à jour initiale si tous les agents ont réalisé une mise à jour initiale, si bien que les données de sauvegarde sont déjà complètes sur le Data Vault existant. L'option qui permet de passer la mise à jour initiale ne fait pas partie directement d'une stratégie de Data Vault mais bien de la stratégie de copie référencée. Confirmez qu'une stratégie de Data Vault avec l'option correcte sélectionnée existe (c.-à-d. avec la « mise à jour » initiale désactivée et des paramètres de limitation et de programmation adéquats). Créez une stratégie de copie à cette fin ou modifiez une stratégie existante (auquel cas toutes les stratégies de Data Vault faisant référence à cette stratégie de copie seront touchées).
6. Créez et enregistrez la stratégie de Data Vault pour le Data Vault Web. Quand vous créez un Data Vault, vous devez indiquer le chemin du dossier et dans ce cas, il s'agira du chemin où les données réelles du Data Vault de type partage de fichiers Windows que vous migrez se trouvent. Sélectionnez la stratégie de copie créée à l'étape 5. Définissez les autres options pour la stratégie de Data Vault de la même manière que dans la stratégie de Data Vault de type partage de fichiers Windows originale (paramètres de réseau, paramètres Active Directory).
7. Quand vous êtes certain que les agents sauvegardent les fichiers vers le nouveau Data Vault Web, supprimez la stratégie originale de Data Vault de type partage de fichiers Windows.

Une fois la stratégie enregistrée, les agents recommenceront à copier les données dans le nouveau Data Vault Web à l'aide du protocole HTTPS.

Configuration des options de Data Vaults Web à l'aide de l'interface de ligne de commande (DvConfig)

L'utilisation de cet utilitaire depuis l'interface de ligne de commande permet de changer les paramètres de configuration d'un Data Vault Web tels que les utilisateurs de sauvegarde et administratif et leurs mots de passe, d'importer un nouveau certificat, de modifier un port SSL et de créer un certificat auto-signé.

Avant de modifier le moindre paramètre, vous devez arrêter le serveur Data Vault Web en arrêtant le service Windows du serveur Data Vault de HP Data Protector for PCs.

Après avoir introduit les modifications, redémarrez le service Data Vault Web. Les stratégies mises à jour seront redistribuées aux agents.

REMARQUE : Si vous utilisez `DvConfig` pour modifier le port SSL ou le nom ou le mot de passe de l'utilisateur de sauvegarde sur le serveur Data Vault Web, n'oubliez pas de modifier les stratégies de Data Vault correspondantes sur le Policy Server afin qu'elles correspondent.

Utilisation :

`DvConfig [-adminUser login:password -backupUser login:password] [-h] [-i certfile | -s hostname] [-p port] [-v]`

`-adminUser login:password`
Définit les informations d'identification pour le compte DvAdmin. Si aucun nom d'utilisateur ou mot de passe n'est fourni, la valeur « DvAdmin » par défaut est utilisée.

`-backupUser login:password`
Définit les informations d'identification pour le compte DvBackup. Si aucun nom d'utilisateur ou mot de passe n'est fourni, la valeur « DvBackup » par défaut est utilisée.

`-h`
Imprimer ce message.

-i *certfile*
Importer un certificat existant.

`-p port`Définir le port SSL.

`-s hostname`Créer un certificat auto-signé pour le nom de domaine complet.

`-v`
Imprimer les informations de la version et quitter.

4 Configuration des stratégies de protection de Data Protector for PCs

Configuration initiale après l'installation de Data Protector for PCs

Dès après l'installation de Data Protector for PCs, la fenêtre Configuration initiale dans le Policy Server s'ouvre. Avant de pouvoir configurer des stratégies pour Data Protector for PCs, vous devez réussir deux étapes de configuration :

1. **Définissez ou importez un mot de passe du chiffrement.**

   Pour des raisons de sécurité, il faut définir un mot de passe du chiffrement avant de pouvoir utiliser Data Protector for PCs. Cela garantit le chiffrement de tous les fichiers au niveau de l'ordinateur de l'utilisateur et la transmission de fichiers chiffrés sur le réseau. Le même mot de passe sert à chiffrer les fichiers de tous les utilisateurs et de tous les Data Vaults centraux.

   - Un Data Vault central (défini via la console de Policy Server) utilisera toujours le chiffrement sur la base du mot de passe du chiffrement de Data Protector for PCs.
   - Dans le cas des Data Vaults locaux (définis par des utilisateurs via leur ordinateur), les utilisateurs peuvent décider d'utiliser ou non le chiffrement et choisir leur propre mot de passe.

   Lors de la première installation de Data Protector for PCs, vous devez soit **générer**, soit **importer** un mot de passe avant de pouvoir continuer. Après avoir créé un mot de passe, **exportez-le** pour votre sécurité. Le mot de passe est ainsi enregistré dans un emplacement sécurisé. Vous pouvez l'utiliser plus tard pour l'importation.

   Cliquez sur **Définir la stratégie de chiffrement** pour gérer le mot de passe et suivez les instructions affichées.

   REMARQUE : Une fois qu'un mot de passe a été créé ou importé, vous ne pouvez plus le modifier.

2. **Obtenez une licence pour Data Protector for PCs.**

   Si vous réalisez une évaluation de Data Protector for PCs, vous pouvez l'utiliser pendant 60 jours et offrir une protection à un nombre illimité d'utilisateurs sans obtenir de licences supplémentaires. Quand vous aurez décidé d'acheter Data Protector for PCs, vous devrez accéder au service HP License Key Delivery Service à l'adresse https://webware.hp.com/welcome.asp afin de télécharger une clé de licence que vous pourrez saisir. Vous pouvez acheter les licences suivantes :

   - TA032AA ou TA032AAE pour 100 Agents
   - TA033AA ou TA033AAE pour 1 000 Agents

- TA036AA ou TA036AAE pour 100 Agents plus HP Data Protector Starter Pack Windows (B6961BA ou B6961BAE)

Vous devez saisir une clé de licence permanente avant la fin de la période d'évaluation. Dans le cas contraire, à l'issue des 60 jours, les agents ne seront plus en mesure de copier les données dans les Local Repositories ou les Data Vaults. Toutefois, il sera possible de rétablir les versions de fichiers protégés antérieurement.

Cliquez sur **Gestion des licences** pour gérer les licences, puis sur **Entrer une clé de licence pour les utilisateurs Data Protector for PCs**. Suivez les instructions affichées.

REMARQUE : Les licences sont fournies aux Agents lors de leur installation.

Une fois que vous aurez terminé ces étapes de configuration, vous aurez accès à toutes les fonctionnalités de la console de Policy Server. Si vous avez installé uniquement Data Protector for PCs, configurez les autres éléments de Data Protector for PCs dans l'ordre présenté dans la section suivante.

Configuration initiale

Data Protector for PCs est livré avec des stratégies qui suffisent à la majorité des organisations. Il est conseillé de configurer en premier lieu les stratégies du Data Vault, de copie et de protection des fichiers, puis d'installer votre logiciel agent de Data Protector for PCs sur les ordinateurs de bureau et portables de l'utilisateur.

REMARQUE : Au lieu de configurer de nouvelles stratégies, vous pouvez modifier les stratégies livrées avec Data Protector for PCs. Il suffit simplement de sélectionner **Modifier une stratégie existante** au lieu de **Créer une nouvelle stratégie** à chaque étape.

La configuration des stratégies de protection de votre installation s'opère depuis la console de Policy Server. Les stratégies définies centralement sont diffusées à l'ensemble des agents Data Protector for PCs et exécutées sur l'ordinateur portable ou de bureau de l'utilisateur.

1. Exécutez la console de Policy Server de Data Protector for PCs à la fin de l'Assistant d'installation ou à tout autre moment depuis un navigateur via l'URL :

   `http://`*`policyserver`*`/dpnepolicy/`

   où « *`policyserver`* » représente le nom de votre Policy Server Data Protector for PCs. Vous devez être connecté en tant qu'« administrateur » sur le serveur.

2. **Configurez les stratégies de Data Vaults**.

   Les stratégies de Data Vault définissent la destination (un Data Vault Web ou un partage de fichiers Windows) pour la sauvegarde en continu des fichiers de l'utilisateur couverts par la stratégie. Lorsqu'un fichier est modifié, la version antérieure et la version modifiée peuvent être sauvegardées automatiquement vers une ou plusieurs destinations. Un ou plusieurs Data Vaults peuvent être affectés à chaque groupe d'utilisateurs. Par exemple, vous pouvez définir une stratégie de Data Vault

appelée *Ventes* et l'affecter aux groupes d'utilisateurs *Bordeaux.Ventes*, *Paris.Ventes*, *Strasbourg.Ventes* et *Nice.Ventes*.

- Un Data Vault central (défini via la console de Policy Server) utilisera toujours le chiffrement sur la base du mot de passe du chiffrement de Data Protector for PCs.
- Dans le cas des Data Vaults locaux (définis par des utilisateurs via le logiciel agent), les utilisateurs peuvent décider d'utiliser ou non le chiffrement et choisir leur propre mot de passe.

REMARQUE : *Impératifs pour tous les Data Vaults :*

Data Protector for PCs définira les mêmes droits d'accès (listes de contrôle d'accès) pour les fichiers sauvegardés sur le serveur de fichiers que pour les fichiers d'origine. Cela signifie que les utilisateurs peuvent uniquement récupérer les fichiers sauvegardés s'ils ont accès aux fichiers originaux sur leur ordinateur.

Impératifs pour les Data vaults de type partage de fichiers Windows :

Si vous utilisez des Data Vaults standard de type partage de fichiers Wndows, les partages doivent se trouver sur un serveur de fichiers Windows qui ne doit pas obligatoirement être le même que le Policy Server. Toutefois, si vous vous contentez d'évaluer Data Protector for PCs avec un nombre restreint d'agents installés, il peut être utile d'utiliser le même ordinateur pour le Policy Server et le serveur de fichiers Data Vault.

Pour créer une stratégie de Data Vault

a. Cliquez sur **Stratégies > Data Vaults > Stratégies de Data Vault** dans le volet de navigation gauche.

b. Cliquez sur **Créer une stratégie de Data Vault**.

c. Suivez les instructions affichées. Le processus varie en fonction de votre sélection d'un Data Vault Web ou de type de partage de fichiers Windows.

REMARQUE : Au moment de créer un Data Vault, la longueur du chemin du dossier ou de partage ne doit pas dépasser 66 caractères.

Meilleures pratiques :

Conservez pour l'instant la valeur Par défaut pour la stratégie de copie.

Pour le cleanup de Data Vaults de type partage de fichiers Windows

- Si le Data Vault se trouve sur ce Policy Server, conservez la valeur par défaut du nom de cet ordinateur.
- Si le Data Vault se trouve sur un serveur de fichiers Windows différent, installez le logiciel Cleanup de Data Vault sur le serveur et désignez-le en tant qu'ordinateur de cleanup.

3. **Configurez les stratégies de copie**.

La stratégie de copie limite le nombre de clients qui peuvent copier simultanément dans un Data Vault. Elle définit également les mises à jour du Data Vault initiale et programmée afin de garantir la sauvegarde continue. Un ou plusieurs Data Vaults peuvent être affectés à chaque stratégie de copie.

Les stratégies de copie définissent les éléments suivants :

- Nombre d'Agents qui peuvent copier des fichiers simultanément dans vos Data Vaults.
- Planification pour les mises à jour périodiques qui vérifie si tous les fichiers attendus pour un utilisateur se trouvent dans le Data Vault et qui copie, le cas échéant, tout fichier manquant. Ceci permet de garantir davantage que tous les fichiers utilisateur ont été copiés correctement dans le Data Vault.
- La nécessité de réaliser une **mise à jour initiale** (ou une copie). La mise à jour initiale est requise car lors de l'utilisation normale de Data Protector for PCs, chaque fois qu'un utilisateur modifie un fichier bénéficiant de la protection continue de Data Protector for PCs, seules les informations relatives aux modifications sont copiées dans le Data Vault.

La stratégie de copie par défaut s'applique à tous les Data Vaults pour lesquels aucune stratégie de copie explicite n'est définie. Vous pouvez modifier les paramètres de la stratégie de copie par défaut, mais vous ne pouvez pas la supprimer ou la renommer.

Pour créer une stratégie de copie

a. Cliquez sur **Stratégies** dans le volet de navigation gauche.
b. Cliquez sur **Définir les stratégies de copie**.
c. Cliquez sur **Créer une stratégie de copie**.
d. Suivez les instructions affichées.

Meilleure pratique :

- **Limitation** : définissez la période selon vos heures de bureau habituelles et définissez une limitation inférieure pour les autres périodes.
- **Mise à jour initiale** : autorise la mise à jour initiale pour veiller à ce que tous les fichiers utilisateur couverts par les stratégies de protection des fichiers soient sauvegardés.
- **Mettre à jour les fichiers chaque semaine/mois** : dans la mesure où une mise à jour ne doit pas impliquer de copies de fichier, ou alors très peu, ceci permet aux mises à jour du Data Vault de veiller à ce que tous les fichiers utilisateur protégés par la stratégie soient correctement sauvegardés.

4. **Configurez les stratégies de protection des fichiers**.

Les stratégies de protection des fichiers permettent de définir les fichiers à protéger et la durée de conservation des versions antérieures. Par exemple, vous pouvez

définir une stratégie de protection des fichiers que vous baptiserez *Documents Office* pour les documents Word, les feuilles de calcul Excel et les présentations PowerPoint.

Les fichiers stockés sur les disques durs locaux peuvent être protégés.

Il existe deux types de stratégies :

- **Continuous File Protection**, qui offre une protection en temps réel pour les fichiers chaque fois qu'ils sont enregistrés sur disque ou supprimés. Généralement, tout fichier ou document qui permet de sélectionner l'option **Enregistrer** dans un menu doit être protégé par une stratégie Continuous File Protection.

  Data Protector for PCs propose plusieurs exemples de stratégies. Trois sont sélectionnées par défaut après l'installation : *Documents Office*, *Développement logiciel* et *Documents Web*. Vous pouvez commencer en utilisant ces stratégies ou vous pouvez élaborer vos propres stratégies.

- **Open File Protection**, qui offre une protection des fichiers en « photographiant » périodiquement le fichier (généralement, une fois par heure). En général, tout fichier qui est très volumineux (plus de 100 Mo), ouvert la plupart de la journée ou sans l'option de menu **Enregistrer** doit être protégé par cette méthode. Les fichiers standard de ce type sont les fichiers de messagerie et de base de données.

  Data Protector for PCs propose quatre exemples : *Microsoft Outlook*, *Microsoft Outlook Express*, *Windows Mail* et *Thunderbird*. Vous pouvez commencer en utilisant ces stratégies ou vous pouvez élaborer vos propres stratégies.

  REMARQUE : Data Protector for PCs ne prend pas en charge la sauvegarde des fichiers chiffrés au format EFS avec les stratégies Open File Protection, par conséquent les fichiers .pst ne doivent pas être chiffrés avec EFS.

Pour créer une stratégie de protection des fichiers

a. Cliquez sur **Stratégies** dans le volet de navigation gauche.
b. Cliquez sur **Définir les stratégies de protection de fichiers**.
c. Cliquez soit sur **Créer une nouvelle stratégie de Continuous File Protection** ou **Créer une nouvelle stratégie de Open File Protection**.
d. Suivez les instructions affichées.

REMARQUE : Quand vous créez des stratégies de protection des fichiers et définissez des règles d'exclusion ou d'inclusion, les extensions de fichier ne peuvent pas contenir plus de 9 caractères pour les stratégies Open File Protection et plus de 29 caractères pour les stratégies Continuous File Protection.

S'agissant des stratégies Open File Protection, vous pouvez sélectionner des fichiers sans extension dans les règles d'inclusion. Ceci n'est pas possible pour les stratégies Continuous File Protection.

IMPORTANT : Vous avez défini à ce stade toutes les stratégies de base dont Data Protector for PCs a besoin. Data Protector for PCs est livré avec d'autres stratégies préconfigurées qui sont suffisantes pour la majorité des organisations. Nous vous invitons à commencer à installer les Agents sur les ordinateurs de bureau ou les ordinateurs portables des utilisateurs (voir « Installation d'agents Data Protector for PCs » (page 37)). Plus tard, vous pourrez examiner et configurer les stratégies Data Protector for PCs restantes telles que la stratégie de cleanup, la stratégie de contrôle de l'utilisateur, la stratégie de mise à jour de l'agent et la stratégie de rétention des données pour les rapports.

Configuration des stratégies restantes

1. **Configurez l'accès à Active Directory**.

REMARQUE : *Association de groupes Active Directory aux Data Vaults :* vous pouvez associer des Data Vaults aux groupes Active Directory dans la stratégie de Data Vault. Tous les membres des groupes associés seront sauvegardés dans le Data Vault associé. Il est impossible d'associer des utilisateurs individuels. De plus, si vous associez une unité d'organisation, seuls les groupes au sein de cette unité sont associés. Tout utilisateur qui se trouve directement dans l'unité d'organisation n'est pas associé au Data Vault. La liste des groupes Active Directory peut inclure par erreur des groupes autres que des groupes de sécurité tels que des groupes de distribution par exemple. Ceci étant dit, seuls les groupes de sécurité seront associés au Data Vault.

Plusieurs utilisateurs : si deux ou plusieurs utilisateurs partagent un ordinateur, ils doivent appartenir au même groupe Active Directory.

Si vous souhaitez affecter des Data Vaults par groupe ou unité d'organisation ou si vous voulez générer des rapports par groupe ou unité d'organisation, vous devez configurer le Policy Server de sorte qu'il accède à votre Active Directory.

La configuration de l'accès à Active Directory active l'option **Membres de groupes et d'unités d'organisation** pour les Data Vaults (voir la section « Configuration initiale » (page 24)).

Pour configurer l'accès à Active Directory

a. Cliquez sur **Configuration** dans le volet de navigation gauche.

b. Cliquez **Configurer l'accès à Active Directory**.

c. Suivez les instructions affichées.

2. **Configurez la stratégie de Cleanup**.

   Les Local Repositories de Data Protector for PCs sur les ordinateurs de l'utilisateur et les Data Vaults sur les serveurs de Data Vault doivent être nettoyés périodiquement afin de supprimer les versions qui dépassent la durée de rétention définie dans les stratégies de protection des fichiers.

   Pour configurer la stratégie de Cleanup

   a. Cliquez sur **Stratégies** dans le volet de navigation gauche.

   b. Cliquez sur **Définir la stratégie de cleanup**.

   c. Suivez les instructions affichées.

   Afin que le Data Vault puisse prendre en charge plus d'utilisateurs, exécutez le cleanup uniquement pendant les week-ends, à partir du vendredi soir ou du samedi matin, afin qu'il dispose d'un maximum de temps pour l'exécution :

   a. Ouvrez la page Stratégie de cleanup dans la console d'administration Policy Server et modifiez le paramètre **Planning de Cleanup du Data Vault**.

   b. Décochez toutes les cases, sauf vendredi ou samedi :

   - Pour le vendredi, sélectionnez une heure de début tard dans la soirée, par exemple 22h00.
   - Pour le samedi, choisissez une heure de début tôt le matin, par exemple 1h00.

   Quand le cleanup a lieu uniquement les week-ends :

   - La liste des fichiers présentés pour la restauration depuis un Data Vault sera dépassée d'une semaine maximum. Les utilisateurs peuvent toujours lancer l'analyse manuelle des données dans le Data Vault afin d'obtenir un aperçu à jour.
   - Les versions sauvegardées existeront toujours au-delà de la conservation prévue jusqu'à une semaine maximum car le cleanup est réalisé uniquement les week-ends.
   - La gestion des quotas n'est pas à jour. Si les utilisateurs ont dépassé leur quota, il se peut qu'ils doivent attendre jusque la fin du cleanup afin d'avoir à nouveau de l'espace sur le Data Vault. D'un autre côté, il se peut que le dépassement du quota ne soit pas reconnu immédiatement par le système car la génération de rapports sur l'utilisation de l'espace fait partie du processus de cleanup.

Meilleure pratique :

- **Planning de Cleanup du Local Repository** : conservez la valeur par défaut d'une heure.
- **Planning de Cleanup du Data Vault** : la valeur par défaut « nettoyer tous les jours à minuit » devrait convenir à la majorité des installations. Voir la section « Recommandations pour le dimensionnement » (page 32) pour obtenir des informations complémentaires sur la capacité du Data Vault.
- Vous pouvez configurer DPNECleanup de sorte qu'il utilise plusieurs threads de manière renouvelable et réutilisable afin d'utiliser au mieux le CPU et le disque et de permettre ainsi le stockage de plus de données. Voir le « Configuration d'un cleanup à plusieurs threads » (page 35).

3. **Configurez la stratégie de contrôle de l'utilisateur**.

   La stratégie de contrôle de l'utilisateur permet de déterminer le niveau de contrôle des utilisateurs sur les stratégies d'entreprise disponibles sur leur ordinateur.

   Pour configurer la stratégie de contrôle de l'utilisateur

   a. Cliquez sur **Stratégies** dans le volet de navigation gauche.
   b. Cliquez sur **Définir la stratégie de contrôle de l'utilisateur**.
   c. Suivez les instructions affichées.

   Meilleure pratique :

   définissez **autoriser le contrôle de l'utilisateur** sur **Récupération en libre-service**.

4. **Configurez la stratégie de mise à jour de l'agent**.

   La stratégie désigne la version de l'Agent Data Protector for PCs que tous les ordinateurs de bureau et portables protégés par Data Protector for PCs doivent utiliser. La mise à jour à cette version est automatique.

   Pour configurer la stratégie de mise à jour de l'agent

   a. Cliquez sur **Stratégies** dans le volet de navigation gauche.
   b. Cliquez sur **Définir la stratégie de mise à jour de l'agent**.
   c. Suivez les instructions affichées.

5. **Configurez la rétention des données pour les rapports**.

   Cette opération définit la durée de conservation des données pour les rapports de chacune des catégories d'information principales.

   Pour configurer la rétention des données pour les rapports

   a. Cliquez sur **Configuration** dans le volet de navigation gauche.
   b. Cliquez sur **Configurer la rétention des données pour les rapports**.
   c. Suivez les instructions affichées.

Autres tâches de configuration

Ces tâches sont exécutées en général lors de la première installation de Data Protector for PCs.

Obtenez une licence pour votre logiciel Data Protector for PCs.

Si vous réalisez une évaluation de Data Protector for PCs, vous pouvez l'utiliser pendant 60 jours et offrir une protection à un nombre illimité d'utilisateurs sans obtenir de licences supplémentaires. Quand vous aurez décidé d'acheter Data Protector for PCs, vous devrez accéder au service HP License Key Delivery Service à l'adresse https://webware.hp.com/welcome.asp afin de télécharger une clé de licence que vous pourrez saisir.

Pour saisir une clé de licence

1. Cliquez sur **Gestion des licences** dans le volet de navigation gauche.
2. Cliquez sur **Entrer une clé de licence pour les utilisateurs de HP Data Protector for PCs**.
3. Suivez les instructions affichées.

Si vous devez saisir plusieurs licences, vous pouvez créer un fichier texte qui reprend une chaîne de clé de licence par ligne. Vous pourrez ensuite importer le fichier via le champ Importer les clés de licence.

REMARQUE : Les licences sont fournies aux Agents lors de leur installation.

Déplacement de licences

Si vous devez modifier l'adresse IP du Policy Server afin de déplacer le serveur vers un autre système ou si vous devez déplacer les licences depuis un Policy Server vers un autre, contactez le HP Licence Key Delivery Service à l'adresse https://webware.hp.com/welcome.asp.

Définissez, importez ou exportez un mot de passe du chiffrement.

Pour des raisons de sécurité, il faut définir un mot de passe du chiffrement avant de pouvoir utiliser Data Protector for PCs. Cela garantit le chiffrement de tous les fichiers au niveau de l'ordinateur de l'utilisateur et la transmission de fichiers chiffrés sur le réseau. Le même mot de passe sert à chiffrer les fichiers de tous les utilisateurs et de tous les Data Vaults centraux.

- Un Data Vault central (défini via la console de Policy Server) utilisera toujours le chiffrement sur la base du mot de passe du chiffrement de Data Protector for PCs.
- Dans le cas des Data Vaults locaux (définis par des utilisateurs via leur ordinateur), les utilisateurs peuvent décider d'utiliser ou non le chiffrement et choisir leur propre mot de passe.

Lors de la première installation de Data Protector for PCs, vous devez soit générer, soit importer un mot de passe avant de pouvoir continuer. Après avoir créé un mot de passe, exportez-le pour votre sécurité. Le mot de passe est ainsi enregistré dans un emplacement sécurisé. Vous pouvez l'utiliser plus tard pour l'importation.

REMARQUE : Une fois qu'un mot de passe a été créé ou importé, vous ne pouvez plus le modifier.

Pour gérer le mot de passe du chiffrement

1. Cliquez sur **Stratégies** dans le volet de navigation gauche.
2. Cliquez sur **Stratégie de chiffrement**.
3. Suivez les instructions affichées.

Définition du nombre de Agents qui peuvent être pris en charge

Il est difficile de fournir des règles générales qui seront vérifiées dans tous les environnements. Par conséquents, les cas présentés ici décrivent clairement le contexte dans lequel les chiffres donnés sont valides.

Facteurs touchant la taille

Le dimensionnement d'un environnement Data Protector for PCs est complexe. Parmi les facteurs techniques qui influencent le nombre d'utilisateurs qu'un environnement spécifique peut prendre en charge, citons :

- La puissance de traitement du Data Vault (pour la consolidation nocturne des données de sauvegarde)
- La bande passante de réseau et E/S sur le serveur Data Vault
- L'espace disque sur le serveur Data Vault
- La taille de la base de données SQL sur le Policy Server
- La bande passante de réseau et la puissance de traitement sur le Policy Server.

Les paramètres de configuration de Data Protector for PCs et les modes d'utilisation de l'application déterminent lequel de ces éléments peut créer un goulot d'étrangement dans toute installation :

- Le nombre d'utilisateurs sur un Data Vault.
- Le nombre et la taille des fichiers couverts par les stratégies de protection configurées.
- La fréquence de changement des fichiers protégés.
- Les paramètres de rétention pour les types de fichiers protégés.

Recommandations pour le dimensionnement

Data Vault

À condition de réaliser un cleanup quotidien, un Data Vault doté de 14 To de stockage peut prendre en charge jusqu'à **3 500** Agents si les caractéristiques des données moyennes sont les suivantes :

- Nombre moyen de fichiers protégés : 5000

- Taille moyenne des fichiers protégés sur le disque local : 10 Go
- Taille moyenne total sur le Data Vault (compressé) : 4 Go

Si vous devez protéger en moyenne plus de données que dans cet exemple, il suffit d'augmenter la capacité du disque sur le Data Vault pour obtenir plus d'espace pour les données, mais le Data Vault ne sera plus en mesure de réaliser la consolidation nocturne des données de sauvegarde en temps utiles. Envisagez les possibilités suivantes :

- Exécutez le cleanup du Data Vault uniquement les week-ends. Voir l'étape 2 « Configurez la stratégie de Cleanup » de la section « Configuration des stratégies restantes » (page 28) pour obtenir les détails. Cela devrait porter le nombre d'Agents qui peuvent être pris en charge par un Data Vault à 10 000, pour un disque de 40 To, en tenant compte de caractéristiques de données moyennes identiques.
- Pensez à distribuer les données d'utilisateur final sur plusieurs Data Vaults.

Les caractéristiques du matériel de tels Data Vaults sont les suivantes :

Type de Data Vault	Cleanup quotidien (jusqu'à 3 500 agents)	Cleanup hebdomadaire(jusqu'à 10 000 agents)
Partage de fichiers Windows	3 GHz double coeur, 4 Go de RAM, 14 To d'espace disque	3 GHz double coeur, 4 Go de RAM, 40 To d'espace disque
Data Vaults Web	3 GHz quadruple coeur, 4 Go de RAM, 14 To d'espace disque	3 GHz quadruple coeur, 4 Go de RAM, 40 To d'espace disque

Si vos utilisateurs ont moins de données en moyenne, vous pourrez peut-être héberger un nombre plus élevé d'utilisateurs sur un Data Vault.

REMARQUE : HP conseille vivement de maintenir le système d'exploitation du Data Vault et des données de sauvegarde sur des disques séparés physiquement afin de garantir les meilleures performances.

Les meilleures performances seront obtenues en réalisant une défragmentation à intervalle régulier du disque de Data Vault.

Policy Server

Le volume de trafic généré par le Policy Server dépend directement du nombre de Agents hébergés par le serveur. L'utilisation de la version Express de MS SQL Server reprise dans Data Protector for PCs impose une limite maximum de 4 Go sur la taille de base de données et pas plus de 5 000 agents[1] peuvent être pris en charge.

Si vous devez prendre en charge plus de 5 000 clients dans votre environnement, vous pouvez soit ajouter des Policy Servers, soit remplacer MS SQL Express par une version complète de Microsoft SQL Server. De cette manière, le Policy Server peut monter

1. En utilisant la valeur par défaut de 30 jours pour le paramètre rétention des données pour les rapports sur le Policy Server.

facilement jusqu'à 50 000 Agents. Si vous décidez d'utiliser la version complète de MS SQL Server, pensez à porter la mémoire principale du Policy Server à au moins 3 Go.

Pour des raisons de performances, il est préférable d'exécuter le Policy Server sur un serveur différent du serveur Data Vault. L'exécution sur un même serveur est possible, mais un tel cas de figure est conseillé uniquement dans le cadre d'évaluation.

Il faut faut compter au moins un Policy Server, mais il n'est pas nécessaire d'avoir un nombre égal de Data Vaults et de Policy Servers.

Considérations pour le réseau

REMARQUE : La forte latence n'a aucun effet sur les Data Vaults Web. Ce qui suit concerne uniquement les Data Vaults de type partage de fichiers Windows.

En général dans les Data Vaults de type partage de fichiers Windows, HP déconseille de réaliser une mise à jour initiale depuis les Agents de Data Protector for PCs vers les Data Vaults si la latence du réseau entre les deux est supérieure à 50 ms. Ceci est généralement le cas dans les bureaux à domicile ou les bureaux distants qui utilisent une connexion WAN lente. La mise à jour initiale fonctionnera, mais elle durera très longtemps.

Si votre environnement est composé de bureaux en divers endroits et si la latence de réseau pour certains d'entre eux est supérieure à 50 ms, envisagez d'installer les Data Vaults sur plusieurs sites afin que tous les bureaux puissent atteindre au moins un Data Vault dont la latence est de 50 ms maximum.

Une fois la mise à jour initiale terminée, les mises à jour peuvent être réalisées depuis n'importe quel emplacement du réseau d'entreprise, voire depuis un bureau à domicile. Ces mises à jour sont en général assez petites et ne devraient pas poser de problèmes, mêmes avec des connexions de réseau lentes.

Si la mise à jour initiale doit être réalisée via une connexion à latence élevée, il faudra peut-être compter sur plusieurs jours pour l'exécution, mais la mise à jour peut dans ce cas être interrompue sans risque. Data Protector for PCs reprendra la mise à jour à l'endroit où celle-ci avait été interrompue dès que la connexion au Data Vault aura été rétablie.

ASTUCE : Si vous ne connaissez pas la valeur de latence entre vos bureaux, utilisez l'instruction `ping` entre un ordinateur à un emplacement et un ordinateur à un autre emplacement. Chaque ping réussi signalera la latence.

5 Configuration d'un cleanup à plusieurs threads

Les performances de `DPNECleanup` limitent le volume de données de sauvegarde utilisateur sur un Data Vault. Vous pouvez le configurer de sorte qu'il utilise plusieurs threads de manière renouvelable et réutilisable afin d'utiliser au mieux le CPU et le disque et de permettre ainsi le stockage de plus de données.

Dans le cadre du cleanup à plusieurs threads, l'argument de programmateur `-s` donne les arguments par défaut `-e -f -u -p -d 1000`, qui reprennent le cleanup à plusieurs threads par défaut et un retard d'1 seconde pour l'adaptateur automatique. Si vous ne souhaitez pas utiliser ces valeurs par défaut, par exemple, pour désactiver l'exécution à plusieurs threads ou pour la régler, supprimer l'argument -s de l'appel du programmateur et ajoutez les arguments CLI individuels.

REMARQUE :

Même si vous souhaitez désactiver le cleanup à plusieurs threads sous certaines circonstances, il est conseillé de conserver `-e -f -u` en tant qu'arguments pour l'appel de Cleanup sur le Data Vault.

Utilisation de DPNECleanup.exe depuis le CLI

L'argument `-p` sur `DPNECleanup.exe` permet à Cleanup d'initialiser et de démarrer le moteur parallèle et d'autoriser ainsi l'exécution à plusieurs threads. Le moteur parallèle offre sept arguments de ligne de commande facultatifs. Le fichier exécutable DPNECleanup est capable de récupérer ces arguments et de les transmettre au moteur parallèle.

DPNECleanup sera exécuté en mode série si `-p` n'est pas défini. Dans ce mode, le moteur parallèle n'est pas du tout utilisé.

dpnecleanup

`–a` *`affinité`*
Règle l'affinité du processeur sur le nombre donné. Ce nombre représente les bits définis de coeurs de CPU que les threads vont utiliser.

`d` *`retard`*Règle le retard en millisecondes avant le début du fonctionnement de l'adaptateur automatique, laissant le temps au moteur parallèle de démarrer un certain nombre de threads et de créer de l'utilisation système. Par défaut, l'argument `–s` entraîne un retard de 1 000 millisecondes ou 1 seconde.

`–m` *`maxCpuUsage`*
Définit l'utilisation maximum du CPU souhaitée (sur tous les coeurs définis par *`affinité`*) sur le pourcentage *`maxCpuUsage`* que l'adaptateur automatique tentera d'atteindre. *`maxCpuUsage`* doit être un entier compris entre 1 et 100. La valeur par défaut est ‘0’, ce qui signifie pas de limite (le CPU est utilisé complètement).

`–o`

Ressources constantes. L'adaptateur automatique est désactivé et le moteur parallèle ne modifiera pas le nombre de threads simultanées. Utilisez l'argument `-r` pour régler le nombre de threads simultanées. Les arguments `-d`, `-m` et `-q` sont ignorés lors de l'exécution avec `-o`.

`-p`
Permet le Cleanup à plusieurs threads.

`-q` *`maxQueueLength`*
Définit la longueur de file d'attente de disque moyenne maximum souhaitée que l'adaptateur automatique tentera d'atteindre. La valeur doit être un nombre flottant. La valeur par défaut est 2.0.

`-r` *`resourceCount`*
Définit le nombre de ressources simultanées (threads) sur le nombre donné. Par défaut et en association avec l'option `-o`, le système fonctionnera avec 2^(nombre de processeurs) threads simultanées. Si l'adaptateur automatique est exécuté, la valeur donnée représente la limite de ressources simultanées en termes de threads. Ici, la valeur par défaut pour le nombre maximum est '0', ce qui signifie qu'il n'y a pas de limites.

`-z [Idle|BelowNormal|Normal|AboveNormal|High|Realtime]`
Définit la priorité du processus pour toutes les threads. La valeur par défaut est `Normal`.

`-s`
Cleanup du serveur. Définit le Cleanup pour tous les Data Vaults, centraux ou définis par l'utilisateur. Dans le cadre du comportement à plusieurs threads, il est remplacé par les arguments '`-e -f -u -p -d 1000`' quand la commande est exécutée.

`-e`
Cleanup d'entreprise. Définit le cleanup pour tous les Data Vaults centraux définis par les stratégies du Policy Server.

`-f`
Cleanup rapide. Normalement, le cleanup d'agent est exécuté uniquement si le système est inactif. Cette option permet au Cleanup de commencer à tout moment.

`-u`
Cleanup définit par l'utilisateur. Définit le Cleanup pour tous les Data Vaults locaux définis par des stratégies locales créées par l'utilisateur.

6 Installation d'agents Data Protector for PCs

REMARQUE : Les licences sont fournies aux Agents lors de leur installation.

Les agents Data Protector for PCs peuvent être installés de deux manières :

- Individuellement sur chaque ordinateur client. Voir la section « Installation d'Agents Data Protector for PCs sur des ordinateurs clients individuels » (page 37).
- Déployés dans l'entreprise depuis un serveur de fichiers accessibles à tous les ordinateurs client. Voir la section « Déploiement de Agents Data Protector for PCs dans l'entreprise. » (page 38).

Installation d'Agents Data Protector for PCs sur des ordinateurs clients individuels

Configuration requise

Le logiciel Agent Data Protector for PCs peut être installé sur les ordinateurs de bureau et les ordinateurs portatifs d'utilisateur sous Windows. Pour connaître les plateformes prises en charge, consultez la matrice de prise en charge.

Vous devez être connecté sous un compte possédant des autorisations d'administrateur.

Procédure d'installation

1. Insérez le CD-ROM d'installation de Data Protector for PCs. Un Assistant d'installation doit démarrer automatiquement. Si ce n'est pas le cas, exécutez-le manuellement en double-cliquant sur `setup.hta` à la racine du CD-ROM d'installation.
2. Cliquez sur **Installer ou mettre à jour le logiciel Agent de Data Protector for PCs**. Choisissez **Ouvrir** (ou **Exécuter**) si une boîte de dialogue « Ouvrir ou Enregistrer » apparaît.
3. Si Microsoft Windows Installer 3.1 ou version ultérieure n'est pas installé sur l'ordinateur de l'utilisateur, l'Assistant propose de l'installer. Lorsque la boîte de dialogue Mettre à jour Windows Installer s'affiche, cliquez sur **OK** pour l'installer.
4. Si Microsoft .NET Framework 2.0 SP1 ou version ultérieure n'est pas installé sur l'ordinateur de l'utilisateur, l'Assistant propose de l'installer. Lorsque la boîte de dialogue Installer Microsoft .NET Framework 2.0 SP1 s'affiche, cliquez sur **OK** pour l'installer.
5. L'Assistant installe automatiquement l'Agent Data Protector for PCs. Suivez les instructions affichées à l'écran. Lors de l'installation, vous devez saisir les détails du Policy Server.

6. Une fois l'installation et la configuration terminées, cliquez sur **Terminer**. Si une stratégie Open File Protection est définie sur le Policy Server, vous devez redémarrer le système.

   Une icône Data Protector for PCs devrait apparaître désormais dans la barre des tâches (une des icônes suivantes en fonction de l'état de votre protection : ).

7. Vérifiez que l'Agent Data Protector for PCs fonctionne correctement :
   a. Sélectionnez ou créez un fichier test tel qu'un document Word ou une feuille de calcul Excel, par exemple, sur le Bureau. Introduisez-y quelques modifications, puis cliquez sur **Enregistrer**.
   b. Cliquez avec le bouton droit sur le fichier test sur le Bureau, dans l'Explorateur Windows ou dans une boîte de dialogue Ouvrir. Vous devez voir trois entrées Data Protector for PCs dans le menu qui s'affiche (**Rechercher et récupérer des fichiers...**, **Copier la version** et **Ouvrir la version avec *XXX*...**).
   c. Sélectionnez **Ouvrir la version avec *XXX*...** et une liste de versions horodatées du document que vous venez de créer ou de modifier devrait s'afficher. Si vous sélectionnez l'une des versions, elle sera ouverte en tant que document en lecture seule dans l'application appropriée. Ceci est la manière dont un utilisateur récupère une version précédente de ses documents depuis le référentiel Data Protector for PCs local.
8. Répétez les étapes 1 à 8 pour les autres ordinateurs de bureau ou ordinateur portables que vous souhaitez protéger à l'aide de Data Protector for PCs.

Déploiement de Agents Data Protector for PCs dans l'entreprise.

Vous pouvez déployer au départ les Agents Data Protector for PCs dans une Entreprise à l'aide du kit de déploiement de Agent Data Protector for PCs repris sur le CD-ROM d'installation.

REMARQUE : Ce kit de déploiement ne peut être utilisé sur des ordinateurs Vista avec la fonction contrôle de compte d'utilisateur activée (UAC). Pour résoudre ce problème, désactivez UAC ou installez l'Agent de façon interactive.

Dans la procédure décrite ci-après, vous commencez par copier le kit de déploiement de Agent Data Protector for PCs depuis `CD-ROM:\Agent` vers un répertoire du serveur de fichiers accessible à tous vos utilisateurs. Ensuite, vous créez un fichier de paramètre dans ce répertoire à l'aide de `SetupConfig.exe`. Enfin, vous définissez un mécanisme pour exécuter `StartInstall.exe` dans le répertoire partagé depuis l'ordinateur de chaque utilisateur. Par exemple, vous pouvez utiliser un script de connexion. Vous pouvez ensuite contrôler le déploiement à l'aide du rapport sur le déploiement du Agent accessible via la console du Policy Server de Data Protector for PCs.

Contenu du kit

Le kit de déploiement de Data Protector for PCs contient les composants suivants :

`SetupConfig.exe`	Crée et modifie le fichier d'initialisation.
`StartInstall.exe`	Lance `Setup.exe` en tant qu'utilisateur privilégié.
`Setup.exe`	Installe les prérequis et `DataProtectorNE.ini`.
`DataProtectorNE.msi`	Ensemble Windows Installer Data Protector for PCs pour installer le logiciel Agent.
`DataProtectorNE64.msi`	Ensemble Windows Installer Data Protector for PCs pour installer le logiciel Agent sur les ordinateurs 64 bits.
`DataProtectorNE*.*.mst`	Ensemble Windows Installer Data Protector for PCs pour installer la version localisée du logiciel Agent.
`WindowsInstaller.exe`	Met à jour Windows Installer (requis pour l'installation de .NET).
`NetFx20SP1_x64.exe`, `NetFx20SP1_x86.exe`	Installe NET Framework 2.0 SP1.
`Setup.ini`	Fichier de paramètre de l'installation de Data Protector for PCs. Ce fichier sera créé à l'aide de `SetupConfig.exe` (cf. étapes 4 ci-dessous).

Procédure de déploiement et d'installation

1. Copiez les fichiers depuis le répertoire Agent du CD-ROM de distribution vers un répertoire qui est accessible à tous les utilisateurs qui ont l'intention d'utiliser le kit de déploiement de Agent Data Protector for PCs. Il peut s'agir du répertoire d'un partage netlogon commun tels que `\\votreserveur\DPNEDeploy`.
2. Assurez-vous que le nouveau répertoire contient les fichiers repris ci-dessus. Vous pouvez supprimer tous les autres fichiers.
3. Ouvrez une fenêtre de commande DOS (`cmd.exe`) et exécutez l'instruction `cd` pour accéder au répertoire créé à l'étape 1.
4. Exécutez `SetupConfig.exe` pour créer ou modifier le fichier de paramètre `Setup.ini`. La première fois que vous exécutez `SetupConfig.exe`, vous devez saisir des valeurs pour tous les paramètres. Ensuite, vous pourrez exécuter `SetupConfig.exe` à plusieurs reprises pour modifier les paramètres. Si vous ne souhaitez pas modifier un paramètre, appuyez simplement sur la touche **Retour**.

   Les paramètres obligatoires sont :

   - **Chemin d'accès UNC aux packages d'installation** : le chemin d'accès complet au répertoire partagé dans lequel les fichiers ont été copiés à l'étape 1 tel que `\\votreserveur\DPNEDeploy`.
   - Le nom du **Policy Server Data Protector for PCs**. Il peut s'agir d'un nom NetBIOS tel que `VOTRESERVEUR` ou d'un nom de domaine complet comme `votreserveur.votresociété.com`.
   - **Nom d'utilisateur** : le nom d'utilisateur d'un utilisateur possédant des privilèges d'administration sur les ordinateurs qui utilisent le kit de déploiement de Agent

Data Protector for PCs comme un membre du groupe Domain Admins. Il s'agit en général d'un nom d'utilisateur complet reprenant également le domaine tel que `VOTRESOCIÉTÉ\JerryAdmin`.

- **Mot de passe** : le mot de passe associé au nom d'utilisateur. Vous devez le taper deux fois pour le confirmer.

5. Sur l'ordinateur client, exécutez `StartInstall.exe`, par exemple `\\votreserveur\DPNEDeploy\StartInstall`. `Setup.exe` sera ensuite exécuté en arrière-plan, suivant une priorité faible, sous le nom d'utilisateur et le mot de passe définis dans `Setup.ini`. Cela peut faire partie d'un script de connexion. Sachez que vous ne pouvez pas l'inclure dans un script de démarrage car le compte de l'ordinateur n'a pas les autorisations de réseau suffisantes.
6. `Setup.exe` détermine si l'ordinateur client peut prendre en charge Data Protector for PCs. Pour connaître les plateformes Windows prises en charge, consultez la matrice de prise en charge.
7. `Setup.exe` détermine si.NET Framework version 2.0 SP1 est installé. Si ce n'est pas le cas, l'installation a lieu et vous devrez peut-être redémarrer l'ordinateur.
8. `Setup.exe` détermine si Data Protector for PCs est déjà installé. Si ce n'est pas le cas ou si la version est dépassée, il installe Data Protector for PCs.

REMARQUE :

Toute erreur aux étapes 4 à 7 engendrera la consignation d'un message dans le Policy Server de Data Protector for PCs et dans le journal des événements de l'application sur l'ordinateur local.

Vous pouvez contrôler la progression de votre déploiement du Agent à l'aide de la console de Policy Server de Data Protector for PCs :

1. Connectez-vous à la console de Policy Server de Data Protector for PCs.
2. Sélectionnez l'option **Déploiement de Agent** sous **Rapports** dans le volet de navigation gauche.

   Une synthèse du déploiement initial jusqu'à ce jour s'affiche. Elle indique les éléments suivants :

   - Le nombre d'ordinateurs sur lesquels le déploiement est **terminé**.
   - Le nombre d'ordinateurs sur lesquels le déploiement est **en cours**.
   - Le nombre d'ordinateurs où le déploiement a **échoué**.
3. Cliquez sur un chiffre dans la colonne **Nombre d'ordinateurs** afin d'afficher une liste des ordinateurs dans l'état de déploiement sélectionné.

   L'état actuel de chaque ordinateur est affiché. Par exemple, si le déploiement a échoué sur une machine en particulier, la colonne **Informations** indique l'erreur qui s'est produite. Vous pouvez obtenir des détails complémentaires sur un ordinateur en cliquant sur son nom NETBIOS.

7 Mise à jour de Data Protector for PCs

Si vous mettez à jour une version 6.*x* de Data Protector for PCs à la version 7.0, procédez comme suit :

1. Mettez le Policy Server à jour à la version 7.0. Voir la section « Mise à jour du Policy Server » (page 41).
2. Installez le serveur Data Vault Web. Voir le « Installation, configuration et maintenance du serveur Data Vault Web » (page 18).
3. Mettez les agents à jour à la version 7.0.

   Vous pouvez également les mettre à jour à l'aide de la mise à jour manuelle ou de manière silencieuse à l'aide de la stratégie de mise à jour de l'agent. Voir la section « Mise à jour des agents » (page 41) pour les détails.

Mise à jour du Policy Server

Vous pouvez mettre à jour une installation existante de Policy Server de Data Protector for PCs en suivant la procédure d'installation standard. Toutes les configurations existantes (configuration de Data Vault, licences, etc.) seront disponibles dans la version plus récente.

Mise à jour du Policy Server

1. Insérez le CD-ROM d'installation de Data Protector for PCs. Si l'Assistant d'installation ne démarre pas automatiquement, exécutez-le manuellement en double-cliquant sur `setup.hta` à la racine du CD-ROM d'installation.
2. Cliquez sur **Installer le Policy Server** dans la page Installer Data Protector for PCs de l'Assistant pour lancer la mise à jour.
3. Suivez les instructions affichées à l'écran.
4. La procédure d'installation détectera la présence éventuelle d'une installation existante de Policy Server et proposera une mise à jour.
5. Suivez les instructions affichées à l'écran.
6. Une fois l'installation terminée, cliquez sur **Suivant**. Vous pouvez décider ensuite d'exécuter la console de Policy Server de Data Protector for PCs.

REMARQUE : Si le logiciel Cleanup est installé sur le Policy Server, vous devez le mettre à jour également. Vous pouvez réaliser cette opération manuellement ou à l'aide de la stratégie de mise à jour de l'agent.

Mise à jour des agents

Si vous mettez à jour la version de Data Protector for PCs Server, les agents existants qui utilisent la version antérieure de Data Protector for PCs continueront à fonctionner. Vous pouvez également les mettre à jour à l'aide de la mise à jour manuelle ou de manière silencieuse à l'aide de la stratégie de mise à jour de l'agent.

REMARQUE : Après la mise à jour, tous les agents doivent redémarrer afin de pouvoir utiliser les nouveaux Data Vaults Web. L'instruction est fournie via les messages contextuels dans la barre de tâches et via l'onglet Récapitulatif du volet Intégrité de Data Protector for PCs sur les ordinateurs.

Mise à jour automatique de l'agent à l'aide de la stratégie de mise à jour de l'agent

Les agents peuvent être mis à jour de manière silencieuse via la stratégie de mise à jour de l'agent sur le Policy Server. Le package d'installation sera remis automatiquement à tous les clients connectés et la mise à jour sera terminée de manière complètement automatique. L'utilisateur final ne sera pas perturbé.

1. Dans la console de Policy Server, choisissez l'option **Stratégies->Stratégie de mise à jour de l'agent**.
2. Si vous veniez de mettre à jour votre Policy Server, la procédure d'installation a chargé une nouveau package de mise à jour d'agent. Dans la console de Policy Server, cette nouvelle version n'est pas encore sélectionnée.

   Sélectionnez la nouvelle version de l'agent pour rendre la version disponible.
3. En réglant la limitation, vous pouvez régler le nombre maximum de mises à jour autorisées par minute.
4. Cliquez sur **Enregistrer la stratégie de mise à jour de l'agent**.
5. Les agents seront mis à jour maintenant automatiquement jusque la version la plus récente. Les agents de cleanup seront également mis à jour automatiquement.

REMARQUE : Vous pouvez vérifier la progression de la mise à jour de l'agent via le rapport : « Déploiement de l'agent »

Mise à jour manuelle de l'agent

Un agent Data Protector for PCs existant peut être porté à une version plus récente via la procédure d'installation standard.

Avant de passer à une version plus récente de l'Agent, assurez-vous que la version de l'Agent est compatible avec la version du Policy Server Data Protector for PCs.

1. Insérez le CD-ROM d'installation de Data Protector for PCs. Si l'Assistant d'installation ne démarre pas automatiquement, exécutez-le manuellement en double-cliquant sur `setup.hta` à la racine du CD-ROM d'installation.
2. Cliquez sur **Installer l'Agent** dans la page Installer Data Protector for PCs de l'Assistant pour lancer la mise à jour.
3. Suivez les instructions affichées à l'écran.
4. La procédure d'installation détectera la présence éventuelle d'une installation existante de l'Agent et proposera une mise à jour.
5. Suivez les instructions affichées à l'écran.

8 Comment obtenir l'assistance pour Data Protector for PCs

Data Protector for PCs est accompagné d'une année de maintenance. Lors de cette année, vous avez droit aux services suivants :

- Assistance téléphonique, pour parler à un technicien.
- Mises à jour de Data Protector for PCs Server et du logiciel Agent Data Protector for PCs. Vous pouvez télécharger les versions les plus récentes ou une image du CD-ROM depuis le site Web de Data Protector. Accédez à l'adresse http://www.hp.com/go/dataprotector.

Glossaire

Active Directory
(Terme propre à Windows) Le service d'annuaire dans un réseau Windows. Il contient les informations relatives aux ressources du réseau et les rend accessibles aux utilisateurs et aux applications. Les services d'annuaire constituent une méthode cohérente pour nommer, décrire, localiser, gérer les ressources et y accéder quel que soit le système physique sur lequel elles se trouvent.

Agent
Logiciel Data Protector for PCs exécuté sur chaque ordinateur de bureau ou ordinateur portable de l'utilisateur. Il communique avec le Policy Server via les services Web (SOAP et XML) sur le port TCP 80.

console
La console Web permet de définir les stratégies Data Protector for PCs de manière centralisée. Vous devez appartenir au groupe Administrateurs.

Continuous File Protection
Continuous File Protection est la méthode Continuous Data Protection de Data Protector for PCs, qui stocke automatiquement les modifications dans un fichier chaque fois que ce dernier est enregistré. Elle s'applique à la plupart des fichiers de données que l'utilisateur enregistre (par opposition aux fichiers toujours ouverts comme les bases de données ou les fichiers Outlook). Chaque stratégie Continuous File Protection protège un groupe de fichiers qui sont d'une certaine manière en rapport les uns avec les autres. Data Protector for PCs est livré avec des stratégies préconfigurées pour les types de fichier les plus souvent utilisés comme les documents Office et les images. Vous pouvez modifier ces stratégies de protection des fichiers ou créer vos propres stratégies. La stratégie définit également la durée de conservation des versions antérieures des fichiers protégés.

Data Vault
Deux types de Data Vaults sont disponibles :

- Data Vaults Web. Ils utilisent le protocole HTTPS et offrent le meilleur niveau de sécurité pour la transmission de données entre les PC client et le Data Vault et un meilleur rendement dans les environnements à forte latence. C'est pour cette raison qu'ils sont recommandés.
- Data vaults de type partage de fichiers Windows. Il s'agit de dossiers partagés sur un serveur de fichiers où les fichiers sont stockés conformément à la stratégie de Data Vault. Le serveur de fichiers doit prendre en charge le protocole de partage de fichiers Windows (CIFS/SMB). Ils ne conviennent pas aux environnements à forte latence de réseau.

La structure de données des deux types de Data Vault est identique, si bien que vous pouvez convertir les Data Vaults de type partage de fichiers Windows existants en Data Vault Web.

Les utilisateurs peuvent être affectés à une ou plusieurs stratégies de Data Vault en fonction du groupe ou de l'unité d'organisation auquel ils appartiennent.

fichiers protégés
Un fichier protégé est un fichier qui est sauvegardé automatiquement par Data Protector for PCs. Les types de fichiers protégés sont définis dans les stratégies Continuous et Open File Protection.

Local Repository
Le Local Repository est un emplacement de stockage sécurisé sur les ordinateurs Agent et qui sert à stocker des fichiers protégés et des modifications de fichiers. Il se trouve généralement sur le disque dur. C'est un répertoire système caché. Les utilisateurs peuvent récupérer rapidement une version antérieure via un clic du bouton droit de la souris sur le fichier dans le Bureau, l'Explorateur Windows ou une boîte de dialogue d'ouverture. Les fichiers protégés par les stratégies Continuous File Protection sont conservés dans un répertoire caché sur l'ordinateur local jusqu'à ce qu'ils ne répondent plus aux conditions de la période de rétention. Ceux protégés par les stratégies Open File Protection sont temporairement stockés dans le Version Store local jusqu'à ce qu'ils soient copiés vers le Data Vault. Le chemin d'accès au Local Repository est généralement `C:\{DPNE}`.

mise à jour initiale
Data Protector for PCs protège les fichiers continuellement alors que les utilisateurs les modifient en enregistrant les modifications. Chaque fois qu'un utilisateur crée un Data Vault, Data Protector for

PCs doit réaliser une mise à jour initiale de tous les fichiers protégés de l'utilisateur dans le vault. Les utilisateurs peuvent sélectionner la manière dont la mise à jour initiale sera réalisée : immédiatement ou en arrière-plan.

Open File Protection

Open File Protection sauvegarde les fichiers qui sont toujours ouverts tels que les dossiers personnels Outlook et plusieurs fichiers de base de données en prenant des instantanés des fichiers à intervalle régulier. Ceci s'appelle parfois « quasi » Continuous Data Protection. Une stratégie Open File Protection définit la protection des fichiers ouverts, définis par des ensembles de règles d'inclusion et d'exclusion. Par exemple, vous pouvez définir une stratégie appelée « Dossier personnels Outlook » qui concerne les fichiers .pst Outlook en définissant une règle d'inclusion telle que « se termine par '.pst' ». Si vous souhaitez exclure les fichiers .pst archivés, vous pouvez créer ensuite la règle d'inclusion « contient 'archive' ». Les stratégies définissent également la durée de conservation des versions antérieures des fichiers protégés. Les stratégies Open File Protection s'appliquent à tous les utilisateurs.

Policy Server

Le Policy Server assure la gestion centralisée des stratégies de Data Protector for PCs. Il récupère également les informations relatives au statut dans les Agents et fournit des rapports sur le déploiement et le fonctionnement.

stratégie

Une stratégie est un ensemble de règles définies de manière centralisée dans le Policy Server et exécutée par le Agent sur chaque ordinateur de bureau/ordinateur portable/ordinateur portatif.

Stratégie de cleanup

Les périodes de rétention définies par les stratégies de protection des fichiers sont appliquées par les tâches de cleanup qui sont exécutées périodiquement. La fréquence est définie dans la stratégie de cleanup. Par défaut, le cleanup des Local Repositories de l'utilisateur s'effectue chaque heure, et celui des Data Vaults définis localement une fois par jour. Les Data Vaults de type partage de fichiers Windows centraux sont nettoyés par un ordinateur désigné à l'aide de la stratégie de Data Vault, tandis que les Data Vaults Web sont nettoyés par le cleanup exécuté localement sur le serveur Data Vault. La stratégie de cleanup s'applique à tous les utilisateurs.

Stratégie de contrôle de l'utilisateur

Cette stratégie détermine le niveau de contrôle d'utilisateurs individuels sur le logiciel Agent qui est exécuté sur leur ordinateur de bureau/leur ordinateur portable/leur ordinateur portatif. Vous pouvez verrouiller le Agent de sorte que les stratégies soient complètement masquées, vous pouvez autoriser les utilisateurs à voir les stratégies, mais pas à les modifier ou vous pouvez les laisser ajouter leurs propres stratégies. Vous pouvez définir le niveau de contrôle séparément sur chaque grande stratégie Data Protector for PCs. La stratégie de contrôle de l'utilisateur s'applique à tous les utilisateurs.

Stratégie de copie

Les stratégies de copie définissent les éléments suivants :

- Nombre d'Agents qui peuvent copier des fichiers simultanément dans vos Data Vaults.
- Planification pour les mises à jour périodiques qui vérifie si tous les fichiers attendus pour un utilisateur se trouvent dans le Data Vault et qui copie, le cas échéant, tout fichier manquant. Ceci permet de garantir davantage que tous les fichiers utilisateur ont été copiés correctement dans le Data Vault.
- La nécessité de réaliser une *mise à jour initiale*. La mise à jour initiale est requise car lors de l'utilisation normale de Data Protector for PCs, chaque fois qu'un utilisateur modifie un fichier bénéficiant de la protection continue de Data Protector for PCs, seules les informations relatives aux modifications sont copiées dans le Data Vault.

Si vous avez installé uniquement Data Protector for PCs, il faut définir une stratégie de copie afin de réaliser une mise à jour initiale de tous les fichiers protégés de vos utilisateurs.

Utilisateur administratif

Un utilisateur du serveur Data Vault Web qui s'occupe des tâches d'administration telles que la création et la suppression de Data Vaults et la migration des données de sauvegarde client.

Utilisateur de la sauvegarde

Un utilisateur du serveur Data Vault Web qui exécute des opérations d'utilisateur final telles que la sauvegarde ou la restauration de fichiers.

Index

U

V

W