IBM Spectrum Protect for Virtual Environments
Version 8.1.6

Data Protection for VMware
Guide d'installation

IBM Spectrum Protect for Virtual Environments
Version 8.1.6

Data Protection for VMware
Guide d'installation

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 133.

Cette édition s'applique à la version 8.1.6 d'IBM Spectrum Protect for Virtual Environments (référence produit 5725-X00), ainsi qu'à toutes les éditions et modifications ultérieures jusqu'à indication contraire dans de nouvelles éditions.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Table des matières

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	**IBM Canada**
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

A propos de cette publication

IBM Spectrum Protect for Virtual Environments permet d'effectuer une sauvegarde incrémentielle hors hôte au niveau du bloc ainsi qu'une reprise de fichier et une restauration instantanée depuis une sauvegarde des machines virtuelles complètes pour des machines invitées Windows et Linux. Les sauvegardes incrémentielles au niveau des blocs sont disponibles lorsque vous utilisez IBM Spectrum Protect for Virtual Environments avec le dispositif de transfert de données IBM Spectrum Protect.

Public visé

Cette publication s'adresse aux utilisateurs et aux administrateurs qui souhaitent installer et configurer IBM Spectrum Protect for Virtual Environments.

Le manuel *IBM Spectrum Protect for Virtual Environments : Data Protection for VMware - Guide d'utilisation* contient une présentation générale et décrit les tâches exécutées par l'utilisateur, les scénarios de restauration, les commandes et les messages d'erreur.

Publications

La famille de produits IBM Spectrum Protect inclut IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, IBM Spectrum Protect for Databases et plusieurs autres produits de gestion de l'espace de stockage IBM®.

Pour consulter la documentation produit IBM, voir IBM Knowledge Center.

Nouveautés de la version 8.1.6

IBM Spectrum Protect for Virtual Environments version 8.1.6 inclut de nouvelles fonctionnalités et des mises à jour.

Pour obtenir la liste des nouvelles fonctions et des mises à jour de cette édition et des éditions antérieures à la version 8, voir Mises à jour de Data Protection for VMware.

Les informations nouvelles ou modifiées dans la documentation produit sont signalées par une barre verticale (|) à gauche du changement.

Chapitre 1. Installation et mise à niveau de Data Protection for VMware

L'installation de IBM Spectrum Protect for Virtual Environments inclut la planification, l'installation et la configuration initiale.

Composants installables

Data Protection for VMware inclut plusieurs composants que vous pouvez installer pour protéger votre environnement virtuel.

Selon l'environnement de votre système d'exploitation, les fonctionnalités Data Protection for VMware suivantes sont disponibles pour installation :

Restriction : Chaque module d'installation comporte un fichier de licence utilisateur (EULA). Si vous ne l'acceptez pas, le processus d'installation s'arrête.

Tableau 1. Fonctions Data Protection for VMware disponibles par système d'exploitation

Composant	Linux	Windows
IBM Spectrum Protect Recovery Agent Ce composant fournit des fonctions de montage virtuel et de restauration instantanée.		√
Interface de ligne de commande de Recovery Agent Interface de ligne de commande utilisée pour les opérations de montage.		√
Documents Ces documents incluent le fichier Readme et les fichiers de mentions légales.	√	√
Fichier d'activation de Data Protection for VMware Ce composant permet à IBM Spectrum Protect d'effectuer les types de sauvegarde suivants : • Sauvegarde incrémentielle incrémentielle-permanente • Sauvegarde intégrale incrémentielle-permanente Ce composant est requis pour la protection des applications. Si vous déchargez des charges de travail de sauvegarde, ce fichier doit être installé sur le serveur de sauvegarde vStorage.	√	√

Tableau 1. Fonctions Data Protection for VMware disponibles par système d'exploitation (suite)

Composant	Linux	Windows
Interface graphique de Data Protection for VMware vSphere Ce composant est une interface utilisateur graphique qui accède aux données de la machine virtuelle sur le serveur VMware vCenter. Le contenu de l'interface graphique peut s'afficher dans ces vues : • Une vue de navigateur Web. Cette vue est accessible depuis un navigateur Web à l'adresse de l'hôte du serveur Web. Par exemple : `https://guihost.mycompany.com:9081/TsmVMwareUI/` • La vue du Plug-in client IBM Spectrum Protect vSphere dans le client Web VMware vSphere. Les panneaux de cette vue sont uniquement conçus pour s'intégrer au client Web, mais les données et les commandes de cette vue sont obtenues à partir du même serveur Web d'interface graphique que les autres vues. Le Plug-in client IBM Spectrum Protect vSphere fournit un sous-ensemble des fonctions disponibles dans la vue du navigateur web, ainsi que certaines fonctions supplémentaires. Les fonctions de configuration et de génération de rapports avancés ne sont pas disponibles dans cette vue. Vous pouvez spécifier une ou plusieurs vues lors de l'installation.	√	√
Interface graphique de restauration de fichier Ce composant est une interface graphique Web qui vous permet de restaurer des fichiers à partir d'une sauvegarde de machine virtuelle VMware sans intervention de l'administrateur. L'interface graphique est installée automatiquement lorsque celle de Data Protection for VMware est installée. Elle est activée via l'assistant de configuration.	[1]	√
Dispositif de transfert de données Le dispositif de transfert de données IBM Spectrum Protect transfère des données pour Data Protection for VMware. Cette fonctionnalité est dénommée dispositif de transfert de données. Ce dispositif transfère des données depuis l'environnement virtuel vers le serveur IBM Spectrum Protect. Lorsque vous installez le dispositif de transfert de données sur un serveur, le serveur peut être utilisé comme serveur de sauvegarde vStorage. Vous pouvez installer le dispositif de transfert de données sur le même système que Data Protection for VMware ou sur un autre serveur.	√	√

1. Bien que le composant de l'interface de restauration de fichier doive être installé et activé sur un système Windows, vous pouvez utiliser cette interface pour restaurer des fichiers sur des machines virtuelles invité Windows ou Linux.

2. Le client de sauvegarde-archivage et le dispositif de transfert de données Data Protection for VMware ne peuvent pas être installés sur le même système Windows ou Linux.

Data Protection for VMware décharge la charge de travail de sauvegarde des machines virtuelles vers un serveur de sauvegarde vStorage. Pour réaliser cette tâche, le dispositif de transfert de données V8.1.4 doit être installé sur le serveur de sauvegarde vStorage.

Interface graphique de Data Protection for VMware vSphere

Le composant Interface graphique de Data Protection for VMware vSphere (interface graphique de vSphere) désigne une interface graphique qui permet d'accéder aux données de machines virtuelles sur le serveur VMware vCenter.

Présentation

L'Interface graphique de Data Protection for VMware vSphere est l'interface principale depuis laquelle exécuter les tâches suivantes :

- Lancer ou planifier des sauvegardes de vos machines virtuelles sur un serveur IBM Spectrum Protect.
- Lancer la récupération complète de vos machines virtuelles depuis un serveur IBM Spectrum Protect.
- Générer des rapports sur l'avancement de vos tâches, les événements récents, l'état des sauvegardes et l'utilisation de l'espace. Ces informations peuvent être utilisées pour identifier et résoudre les problèmes liés à la sauvegarde.

Conseil : Des informations sur l'exécution de ces tâches depuis l'interface graphique de vSphere sont disponibles dans l'aide en ligne installée avec l'interface graphique. Cliquez sur **En savoir plus** dans l'une des fenêtres de l'interface pour ouvrir l'aide en ligne et obtenir de l'assistance.

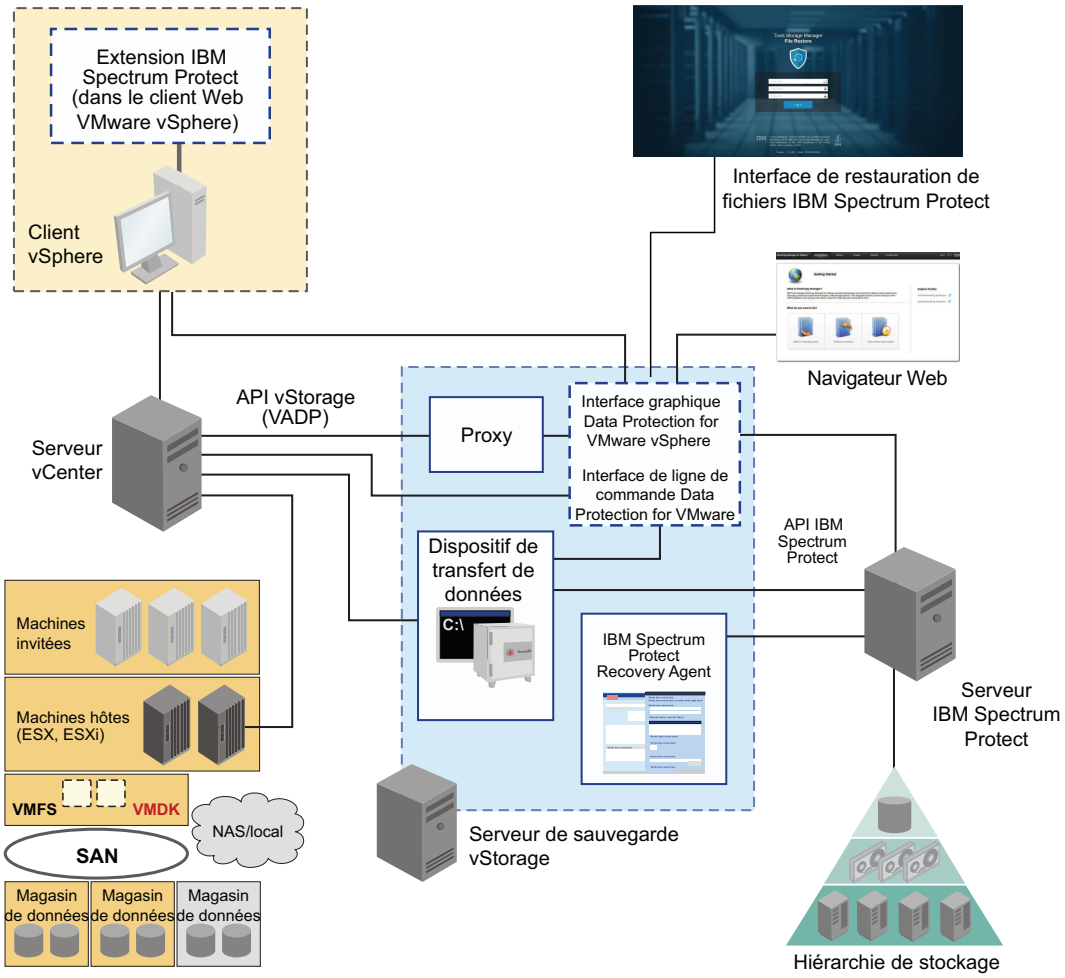

Figure 1. Composants du système Data Protection for VMware dans un environnement utilisateur VMware vSphere

Conditions requises

L'Interface graphique de Data Protection for VMware vSphere peut s'installer sur n'importe quel système satisfaisant aux prérequis du système d'exploitation. Les besoins en ressources de l'interface graphique de vSphere sont minimes puisqu'elle ne traite pas les transferts de données d'E-S.

Conseil : L'installation de l'interface graphique de vSphere sur le serveur de sauvegarde vStorage constitue la configuration la plus courante.

L'interface graphique de vSphere GUI doit disposer d'une connectivité réseau avec les systèmes suivants :

- Serveur de sauvegarde vStorage
- Serveur IBM Spectrum Protect
- Serveur vCenter

De plus, les ports de la base de données Derby (par défaut, `1527`) et du serveur Web de l'interface graphique (par défaut, `9081`) doivent être disponibles.

Configuration

Vous pouvez enregistrer plusieurs interfaces graphiques vSphere sur un même serveur vCenter. Ce scénario diminue le nombre de centres de données (et de leurs sauvegardes d'invités de machine virtuelle) gérés par une interface graphique VMware vSphere unique. Un serveur vCenter peut ensuite gérer un sous-ensemble du nombre total de centres de données définis sur le serveur vCenter.

Pour mettre à jour les centres de données gérés, accédez à **Configuration** > **Modifier la configuration**.

Lorsque vous enregistrez plusieurs interfaces graphiques vSphere sur le même serveur vCenter, les consignes suivantes s'appliquent :

- Chaque centre de données ne peut être géré que par une seule interface graphique vSphere installée.
- Un nom de noeud VMCLI unique est requis pour chaque interface graphique vSphere installée.
- L'utilisation de noms de noeud de dispositif de transfert de données uniques pour chaque interface graphique installée simplifie la gestion des noeuds.

Accès à l'interface graphique de vSphere

L'interface graphique de vSphere est accessible via les méthodes suivantes :

- Une interface autonome intégrée à un navigateur Web. Vous pouvez accéder à cette interface graphique depuis un signet d'URL dirigé vers son serveur Web, par exemple :

  `https://`*`nom_hôte`*`:`*`port`*`/TsmVMwareUI/`

  où :

  – *nom_hôte* désigne le nom du système sur lequel l'Interface graphique de Data Protection for VMware vSphere est installée.

  – *port* désigne le numéro du port à travers lequel l'interface graphique de vSphere est accessible. Par défaut, il s'agit du port 9081.
- Une extension de client Web vSphere se connectant à un serveur Web d'interface graphique pour accéder aux machines virtuelles du stockage IBM (dénommée

extension de protection des données). Le contenu est un sous-ensemble de ce qui est fourni dans l'interface graphique pour navigateur web.

Vous pouvez définir une ou plusieurs méthodes d'accès lors de l'installation.

Windows Le répertoire d'installation par défaut est `C:\IBM\SpectrumProtect\webserver`.

Linux Répertoire d'installation par défaut : `/opt/tivoli/tsm/tdpvmware/common/webserver`.

IBM Spectrum Protect Recovery Agent

Utilisez le service Recovery Agent (agent de récupération) pour monter n'importe quel volume d'instantanés depuis le serveur IBM Spectrum Protect.

Présentation

Vous pouvez utiliser le protocole iSCSI pour accéder un instantané à partir d'un système distant.

Si vous avez besoin d'afficher l'instantané en local avec un accès en lecture seule sur le système client, utilisez Data Protection for VMware version 8.1.4 ou antérieure.

De plus, l'agent de récupération offre à la fois la fonction de restauration instantanée et la protection pour les applications invitées. La restauration instantanée active le volume utilisé pour qu'il reste disponible lorsque l'opération de restauration se poursuit en arrière-plan. La protection d'application active des applications qui sont installées sur une machine virtuelle invitée, par exemple Microsoft Exchange Server ou Microsoft SQL Server, pour qu'elles soient disponibles pour la protection de sauvegarde et de restauration.

L'agent de récupération peut exécuter les tâches suivantes depuis un système distant :

- Collecte d'informations sur les données pouvant être restaurées. Par exemple :
  - Machines virtuelles sauvegardées.
  - Images instantanées disponibles pour une machine virtuelle sauvegardée.
  - Partitions disponibles dans un instantané spécifique.

Pour des informations détaillées sur les commandes, les paramètres et les codes retour, consultez la section de référence sur les commandes dans le *Guide d'utilisation d'IBM Spectrum Protect for Virtual Environments : Data Protection for VMware*.

Conditions requises

Windows Sur les systèmes Windows, l'interface graphique et l'interface de ligne de commande de l'agent de récupération sont installées lors de l'installation complète de Data Protection for VMware ou d'une installation avancée du dispositif de transfert des données.

Accès à l'agent de récupération

Windows Vous pouvez accéder à l'agent de récupération depuis le menu **Démarrer** : **Démarrer** > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect Recovery Agent**.

Plug-in client IBM Spectrum Protect vSphere

Le Plug-in client IBM Spectrum Protect vSphere est une extension du client Web VMware vSphere qui fournit une vue de Web l'interface graphique de Data Protection for VMware vSphere.

Présentation

Le Plug-in client IBM Spectrum Protect vSphere fournit un sous-ensemble de fonctions disponibles dans la vue du navigateur de l'interface graphique de Data Protection for VMware vSphere, ainsi que des fonctions supplémentaires.

Exigence de configuration

Pour installer le Plug-in client IBM Spectrum Protect vSphere, vous devez sélectionner les options suivantes lorsque vous exécutez l'assistant de configuration d'IBM Spectrum Protect for Virtual Environments :

- Sur la page **vCenter Settings** de l'assistant de configuration, sélectionnez **Update Registration** pour enregistrer le plug-in auprès du vCenter associé.
- Saisissez l'adresse hôte de l'interface graphique, ainsi que l'utilisateur et le mot de passe du vCenter.

Une fois l'assistant terminé, le plug-in est enregistré auprès du vCenter.

Accès à l'extension de protection des données

Vous pouvez accéder à cette extension depuis le client Web de vSphere.

Interface de ligne de commande Data Protection for VMware

L'interface CLI de Data Protection for VMware est une interface de ligne de commande toutes fonctions qui s'installe avec l'Interface graphique de Data Protection for VMware vSphere.

Présentation

Vous pouvez utiliser l'interface CLI de Data Protection for VMware pour effectuer les tâches suivantes :

- Lancer ou planifier des sauvegardes de vos machines virtuelles sur un serveur IBM Spectrum Protect.
- Lancer la récupération complète de vos machines virtuelles, fichiers de machines virtuelles ou disques de machines virtuelles (VMDK) depuis un serveur IBM Spectrum Protect.
- Afficher les informations de configuration sur la base de données et l'environnement de sauvegarde.

Bien que l'Interface graphique de Data Protection for VMware vSphere soit l'interface de tâche principale, l'interface CLI de Data Protection for VMware offre une interface secondaire utile.

L'interface CLI de Data Protection for VMware peut, par exemple, être utilisée pour implémenter un mécanisme de planification différent de celui implémenté par l'Interface graphique de Data Protection for VMware vSphere. D'autre part, l'interface CLI de Data Protection for VMware est utile lorsque vous évaluez des résultats de l'automatisation avec des scripts.

Accès à l'Interface de ligne de commande Data Protection for VMware

Vous pouvez accéder à l'interface CLI de Data Protection for VMware depuis une ligne de commande.

Pour des informations détaillées sur les commandes disponibles, consultez la section de référence sur les commandes dans le *Guide d'utilisation d'IBM Spectrum Protect for Virtual Environments : Data Protection for VMware*.

Interface de restauration de fichier de IBM Spectrum Protect

Vous pouvez restaurer des fichiers individuels à partir d'une sauvegarde de machine virtuelle VMware.

Présentation

L'interface de restauration de fichier est une interface Web où vous pouvez restaurer des fichiers individuels depuis une sauvegarde de machine virtuelle. L'avantage de cette interface est que les propriétaires de fichier, de logiciel ou de la plateforme peuvent restaurer leurs propres fichiers sans connaissance préalable des opérations de sauvegarde et de restauration de IBM Spectrum Protect.

La fonction d'interface de restauration de fichiers est installée lorsque vous sélectionnez l'option de protection de vos données dans un environnement vSphere. Pour que cette interface soit disponible, vous devez activer la fonction de restauration de fichier depuis l'assistant de configuration de Data Protection for VMware.

Accès à l'interface de restauration de fichier de IBM Spectrum Protect

Pour accéder à l'interface de restauration de fichier, ouvrez un navigateur Web et entrez l'URL indiquée par votre administrateur. Par exemple :

`https://nom_hôte:9081/FileRestoreUI`

où *nom_hôte* désigne le nom d'hôte du système sur lequel l'Interface graphique de Data Protection for VMware vSphere est installée.

Dispositif de transfert de données

Un dispositif de transfert de données est un composant logiciel Data Protection for VMware qui transfère des données en provenance et à destination du serveur IBM Spectrum Protect.

Présentation

Dans un environnement VMware classique, le dispositif de transfert de données est utilisé pour stocker des sauvegardes de machine virtuelle sur un noeud de centre de données.

Lorsque vous installez Data Protection for VMware, le dispositif de transfert de données est inclus dans l'installation. Le dispositif de transfert de données est installé sur le même système que l'interface graphique Data Protection for VMware vSphere et d'autres composants de Data Protection for VMware.

Vous pouvez également installer des dispositifs de transfert de données sur des systèmes distants, indépendamment des autres composants de Data Protection for VMware, pour redistribuer la charge de sauvegarde entre plusieurs systèmes.

Les opérations de sauvegarde différentielle par image instantanée ne sont pas prises en charge dans l'environnement VMware. Vous ne pouvez pas exécuter d'opérations de sauvegarde différentielle par image instantanée sur un système de fichiers qui réside sur un gestionnaire de fichiers NetApp sur un hôte sur lequel le dispositif de transfert de données Data Protection for VMware est également installé.

Configuration des dispositifs de transfert de données

Pour plus d'informations sur la planification, l'installation et la configuration des dispositifs de transfert de données, reportez-vous à la liste suivante :

Action	Description
Déterminer le nombre de dispositifs de transfert de données nécessaires pour protéger votre environnement vSphere.	Plusieurs noeuds de dispositifs de transfert de données peuvent être nécessaires pour protéger votre environnement vSphere. Pour déterminer le nombre de noeuds de dispositifs de données nécessaires, reportez-vous à la note technique 2007197. Cette note technique inclut également des remarques sur l'utilisation de machines virtuelles ou physiques pour des noeuds de dispositifs de transfert de données et la localité de dispositifs de données.
Installer Data Protection for VMware.	Pour installer Data Protection for VMware, exécutez le programme d'installation de Data Protection for VMware et sélectionnez **Installation standard** sous Windows ou **Complète** sous Linux. Cette option d'installation installe tous les composants de Data Protection for VMware, y compris les dispositifs de transfert de données. Pour plus d'informations sur l'exécution du programme d'installation de Data Protection for VMware, voir «Installation des composants de Data Protection for VMware», à la page 23.

Action	Description
Définir les dispositifs de transfert de données de l'environnement.	A l'issue de l'exécution de l'assistant d'installation de Data Protection for VMware, l'assistant de configuration de l'interface graphique Data Protection for VMware vSphere s'ouvre pour vous permettre de configurer les communications avec le serveur IBM Spectrum Protect. Dans la page Noeuds de dispositif de transfert de données de l'assistant de configuration, définissez les informations des dispositifs de transfert de données locaux et distants que vous souhaitez installer sur des systèmes distincts. Si vous effectuez l'installation sur un système d'exploitation Windows et que vous sélectionnez l'option **Créer des services** lors de la définition du dispositif de transfert de données, les informations de configuration associées sont sauvegardées dans un fichier d'options à l'emplacement suivant : `C:\Program Files\Tivoli\TSM\baclient\` En outre, les services nécessaires au dispositif de transfert de données sont configurés. Si vous installez le dispositif de transfert sur un système d'exploitation Linux ou lancez l'installation sous Windows sans sélectionner l'option **Créer des services** lors de la configuration, vous devez suivre les étapes de la rubrique «Configuration de noeuds de dispositif de transfert de données avec l'interface graphique du plug-in vSphere», à la page 95 pour créer le fichier d'options et configurer les services requis.
Installer et configurer des dispositifs de transfert de données supplémentaires sur des systèmes distants, si nécessaire.	Pour installer un dispositif de données sur un système distant, exécutez le programme d'installation de Data Protection for VMware. Sur les systèmes d'exploitation Windows, sélectionnez l'installation avancée, puis l'option permettant d'installer uniquement la fonction du dispositif de transfert de données dans l'assistant de configuration. Sous Linux, sélectionnez **Personnalisé** dans la liste des types d'installation de l'assistant de configuration. Vérifiez que l'option **Dispositif de transfert de données de Data Protection for VMware** est sélectionnée. Cette option est sélectionnée par défaut. A l'issue de l'installation, suivez les instructions de la rubrique «Configuration de noeuds de dispositif de transfert de données avec l'interface graphique du plug-in vSphere», à la page 95 pour configurer des dispositifs de transfert de données sur des systèmes distants.

Planification de l'installation de Data Protection for VMware

Data Protection for VMware supprime l'impact des sauvegardes en cours d'exécution sur une machine virtuelle en déchargeant les hôtes ESX ou ESXi des charges de travail relatives aux sauvegardes et en les plaçant sur un serveur de sauvegarde vStorage.

Data Protection for VMware fonctionne avec le dispositif de transfert de données pour exécuter des sauvegardes intégrales incrémentielles permanentes et incrémentielles incrémentielles permanentes de machines virtuelles. Le noeud de dispositif de transfert de données "déplace" les données vers le serveur IBM Spectrum Protect afin de stocker les images, puis de les utiliser ultérieurement pour restaurer l'image d'une machine virtuelle. La restauration instantanée est disponible au niveau du volume de disque et au niveau de la totalité d'une machine virtuelle.

Conseil : Le dispositif de transfert de données est un composant sous licence distincte disposant de ses propres interfaces utilisateur et de sa propre documentation. Nous vous recommandons fortement de vous familiariser avec ce produit et sa documentation afin d'intégrer de façon adéquate un plan global de protection de vos machines virtuelles avec Data Protection for VMware. Data Protection for VMware pour Windows 64 bits inclut le dispositif de transfert de données.

Feuille de route d'installation

Le tableau suivant identifie les étapes à exécuter pour réaliser un processus d'installation.

Tableau 2. Tâches d'installation pour les clients Data Protection for VMware nouveaux ou existants

Etape	Tâche	Commencez ici
1	Vérifiez la configuration système requise.	Assurez-vous que le système sur lequel Data Protection for VMware va être installé remplit les conditions requises.
2	Vérifiez les autorisations utilisateur requises.	Evitez les erreurs ou retards potentiels lors de l'installation en utilisant les niveaux de droits requis.
3	Vérifiez la disponibilité des ports de communication requis.	Empêchez tout échec ou retard lors de l'installation en ouvrant les ports de communication requis avant de tenter d'installer Data Protection for VMware.
4	Installez Data Protection for VMware: • Installation de Data Protection for VMware à l'aide de l'assistant d'installation • «Installation des composants de Data Protection for VMware en mode silencieux», à la page 28 Mettez à niveau Data Protection for VMware : Mettre à niveau Data Protection for VMware	Chaque module d'installation comporte un fichier de licence utilisateur (EULA). Si vous ne l'acceptez pas, l'installation se termine.

Tableau 2. Tâches d'installation pour les clients Data Protection for VMware nouveaux ou existants (suite)

Etape	Tâche	Commencez ici
5	«Configuration d'une nouvelle installation à l'aide de l'assistant», à la page 43 Si vous comptez mettre à niveau Data Protection for VMware, d'autres tâches de configuration peuvent être requises selon les composants installés. Pour plus de détails, consultez les rubriques de configuration dans le manuel *IBM Spectrum Protect for Virtual Environments : Data Protection for VMware - Guide de l'utilisateur*.	Utilisez l'assistant de configuration pour une configuration initiale. Selon les fonctions installées, d'autres tâches de configuration peuvent être requises, comme décrit dans cette section.

Conseil : La publication suivante, disponible sur le wiki IBM Spectrum Protect, est destinée à vous aider lors de la planification des hôtes proxy requis pour votre environnement de sauvegarde Data Protection for VMware spécifique :
Step by Step Guide To vStorage Backup Server (Proxy) Sizing
Cette publication est disponible dans la section relative à IBM Spectrum Protect for Virtual Environments.

Scénarios d'installation

Avant d'installer Data Protection for VMware, choisissez le scénario qui répond le mieux aux besoins de votre entreprise.

Vous pouvez installerData Protection for VMware et le dispositif de transfert de données à l'aide de l'interface graphique ou en mode silencieux :

- «Installation des composants de Data Protection for VMware à l'aide de l'assistant d'installation», à la page 24
- «Installation des composants de Data Protection for VMware en mode silencieux», à la page 28

Pour obtenir la liste des fonctions et des composants disponibles par plateforme, voir «Composants installables», à la page 1.

Tableau 3. Scénarios d'installation

Numéro du scénario	Description	Tâches à réaliser
1	Utilisez ce scénario pour une nouvelle installation où vous désirez installer Data Protection for VMware et le dispositif de transfert de données sur le même système.	Windows Vous pouvez utiliser l'outil Suite Installer en mode interface graphique ou en mode silencieux. Linux Vous pouvez utiliser InstallAnywhere en mode interface graphique ou en mode silencieux.

Tableau 3. Scénarios d'installation (suite)

Numéro du scénario	Description	Tâches à réaliser
2	Utilisez ce scénario si vous désirez installer un dispositif de transfert de données (proxy de montage), un agent de récupération et les packages de support requis sur ce système.	Windows Vous pouvez effectuer une installation avancée à l'aide de l'outil Suite Installer. Linux La fonction de transfert de données est à présent installée avec Data Protection for VMware.

Configuration requise

Votre système doit respecter la configuration système appropriée pour pouvoir implémenter des composants Data Protection for VMware.

Configuration logicielle requise

Les détails des exigences en termes de logiciels et de système d'exploitation sont sujets à modification. Pour connaître la configuration logicielle en cours, voir la note technique 1505139.

Configuration matérielle

La configuration matérielle requise varie selon les éléments suivants et en dépend :

- Nombre de serveurs protégés
- Nombre de volumes protégés
- Tailles des jeux de données
- Connectivité LAN et SAN

Remarque : Le composant Recovery Agent ne prend pas en charge les opérations dans un environnement hors réseau local.

Le tableau suivant décrit la configuration matérielle requise pour l'installation de Data Protection for VMware.

Tableau 4. Configuration matérielle requise pour Data Protection for VMware.

Composant	Configuration minimale	Configuration privilégiée
Système	Processeur IntelPentium D 3 GHz Dual Core ou compatible	Non applicable
Mémoire	2 Go de RAM, 2 Go d'espace d'adresse virtuelle	Non applicable
Espace disque dur disponible	200 Mo pour le dossier 'Documents and Settings'	2 Go
Carte NIC	1 NIC - 100 Mb/s	1 NIC - 1 Gb/s

Remarque : En fonction du nombre de processus parallèles, les sauvegardes des machines virtuelles peuvent nécessiter une grande quantité de mémoire.

La mémoire requise peut être étendue via la commande **dsmc backup vm** et peut être calculée à l'aide de la formule suivante :

Mémoire requise = (TailleDisque / TailleMBLK) * TailleMémoireTamponLecture * VMMAXPARALLEL

où :

- **TailleDisque** est la taille du disque invité en cours de traitement.
- **TailleMBLK** est la taille d'un mégabloc. Cette valeur correspond à 128 Mo pour des disques de moins de 2 To et est égale à 1 Go pour des disques de plus de 2 To.
- **TailleMémoireTamponLecture** est la taille de la mémoire interne d'IBM Spectrum Protect utilisée pour prendre en charge les informations MBLK. La taille de la mémoire tampon est 256 ko.
- **VMMAXPARALLEL** représente le nombre maximal de machines virtuelles qui peuvent être sauvegardées au même moment au cours d'une seule opération de sauvegarde.

Par exemple, pour sauvegarder 10 invités, chacun avec des disques de 40 Go et le paramètre VMMAXPARALLEL 2 au cours d'une seule opération de sauvegarde, vous devez disposer des éléments suivants :

- **TailleDisque** = 40 Go = 41943040 ko ;
- **TailleMBLK** = 128 Mo = 131072 ko ;
- **TailleMémoireTamponLecture** = 256 ko ;
- **VMMAXPARALLEL** = 2.

Mémoire requise = (41943040 / 131072) * 256 ko * 2 = 16384 ko = 160 Mo.

Remarque : Pour sauvegarder le même nombre d'invités avec le paramètre 'VMMAXPARALLEL 2' au cours de cinq opérations de sauvegarde parallèles, vous devez disposer (au maximum) de cinq fois plus de mémoire que dans l'exemple précédent, à savoir 800 Mo.

Un hôte proxy Windows est requis pour Recovery Agent sous Linux. Recovery Agent doit être installé sur cet hôte proxy Windows.

Restriction : Les restrictions suivantes s'appliquent aux disques VMDK VMware utilisés dans une opération de sauvegarde :

- Pour le mode de sauvegarde incrémentielle incrémentielle-permanente, chaque disque VMDK concerné par l'opération de sauvegarde ne doit pas être d'une taille supérieure à 2 To. Si cette taille est dépassée, l'opération de sauvegarde échoue. Pour augmenter la taille du disque VMDK au-delà de 2 To, spécifiez la taille maximale avec l'option `vmmaxvirtualdisks`. Pour plus d'informations, recherchez `vmmaxvirtualdisks` dans l'IBM Knowledge Center.
- Pour le mode de sauvegarde intégrale incrémentielle-permanente, chaque disque VMDK concerné par l'opération de sauvegarde ne doit pas être d'une taille supérieure à 2 To. Si cette taille est dépassée, l'opération de sauvegarde échoue.

Pour éviter un éventuel échec dans l'un ou l'autre des modes de sauvegarde, vous pouvez spécifier `vmskipmaxvirtualdisks yes` dans le fichier d'options du dispositif de transfert de données afin que le traitement des disques VMDK soit omis. Pour plus d'informations, voir le Vmskipmaxvirtualdisks.

Prérequis pour la restauration de fichier

Avant de restaurer des fichiers à l'aide de l'interface de restauration de fichier de IBM Spectrum Protect, vérifiez que votre environnement satisfait aux exigences minimales.

Pour activer la fonction de restauration de fichier, Data Protection for VMware doit être installé sur un système Windows.

Prérequis pour la machine virtuelle VMware

Les prérequis suivants concernent la machine virtuelle VMware contenant les fichiers à restaurer :

- Linux Windows VMware Tools doit être installé sur la machine virtuelle.
- Linux Windows La machine virtuelle doit être en exécution lors de l'opération de restauration de fichier.
- Windows La machine virtuelle doit appartenir au même domaine Windows que le système du dispositif de transfert de fichier.
- Windows Si une machine virtuelle est supprimée d'un domaine Windows, puis restaurée ultérieurement, elle doit rejoindre le domaine pour garantir la relation de confiance du domaine. Ne tentez pas d'effectuer une restauration de fichier depuis la machine virtuelle tant que la relation de confiance du domaine n'a pas été rétablie.
- Windows Si l'utilisateur n'est pas le propriétaire du fichier à restaurer, l'autorisation Microsoft Windows `Restaurer des fichiers et des répertoires` doit être affectée à cet utilisateur pour cette machine virtuelle.
- Linux L'authentification d'utilisateur local est requise pour la machine virtuelle. L'authentification n'est pas disponible via les méthodes d'authentification par domaine Windows, par protocole LDAP, Kerberos ou d'autres méthodes d'authentification réseau.
- Linux Sur un système d'exploitation Red Hat Enterprise Linux 6, l'option `ChallengeResponseAuthentication` du fichier de configuration du démon sshd (`/etc/ssh/sshd_config`) doit spécifier YES ou être mise en commentaire. Par exemple, les instructions suivantes sont toutes deux valides :

  ```
  ChallengeResponseAuthentication yes
  #ChallengeResponseAuthentication no
  ```

  Redémarrez le démon sshd après avoir modifié cette option.

Prérequis pour le dispositif de transfert de données

Le dispositif de transfert de données représente un mécanisme spécifique qui "déplace des données" d'un système à un autre.

Windows Le système du dispositif de transfert de données doit appartenir au même domaine Windows que la machine virtuelle qui contient les fichiers à restaurer.

Prérequis pour le proxy de montage

Le système du proxy de montage représente le système proxy Linux ou Windows qui accède aux disques de la machine virtuelle montée via une connexion iSCSI.

Ce système permet aux systèmes de fichiers sur les disques montés des machines virtuelles d'être accessibles à l'interface de restauration de fichiers en tant que points de restauration.

Linux Les systèmes d'exploitation Linux fournissent un démon qui active les groupes de volumes LVM (Logical Volume Manager) lorsque ces volumes deviennent accessibles au système. Configurez ce démon sur le système de proxy de montage Linux de sorte que les groupes de volumes LVM ne soient pas activés lorsqu'ils deviennent disponibles au système. Pour des informations détaillées sur la définition de ce démon, reportez-vous à la documentation Linux appropriée.

Linux Windows Les systèmes proxy de montage Windows et Linux doivent se trouver sur le même sous-réseau.

Configuration requise pour le compte de domaine Microsoft Windows

Les prérequis suivants s'appliquent aux comptes de domaine Windows :

- Windows Les données d'identification de l'administrateur du domaine Windows sont requises pour accéder au partage de réseau. Un administrateur doit entrer ces données d'identification dans l'assistant de configuration de l'Interface graphique de Data Protection for VMware vSphere ou dans le bloc-notes pour activer l'environnement pour les opérations de restauration de fichier.
- Windows Un propriétaire de fichier accède à la machine virtuelle distante (contenant les fichiers à restaurer) à l'aide des données d'identification d'utilisateur du domaine Windows. Ces données d'identification sont saisies dans l'interface de restauration de fichiers lors de la connexion. Les données d'identification de l'utilisateur du domaine vérifient que le propriétaire du fichier est autorisé à se connecter à la machine virtuelle distante et à restaurer des fichiers dans la machine virtuelle distante. Ces données d'identification ne requièrent pas d'autorisations spéciales.
- Windows Si un propriétaire de fichier utilise un compte d'utilisateur de domaine Windows qui limite l'accès à certains ordinateurs (au lieu de pouvoir accéder à tous les ordinateurs sur le domaine), assurez-vous que le système du proxy de montage est inclus dans la liste des ordinateurs accessibles à ce compte d'utilisateur du domaine. Sinon, le propriétaire du fichier ne pourra pas se connecter à l'interface de restauration de fichiers.

Prérequis en matière de bandes magnétiques

La restauration de fichiers depuis une bande magnétique n'est pas prise en charge. La restauration de fichier depuis le stockage sur disque est la méthode privilégiée.

Droits d'installation requis

Avant de lancer l'installation, vérifiez que votre ID utilisateur dispose du niveau de droits requis.

Pourquoi et quand exécuter cette tâche

Tableau 5. Droits d'accès requis pour installer et configurer Data Protection for VMware

Système	Droits requis
Windows	Administrateur
Linux	Superutilisateur

Tableau 5. Droits d'accès requis pour installer et configurer Data Protection for VMware (suite)

Système	Droits requis
Serveur vCenter	Privilèges d'administrateur Le rôle de serveur vCenter nécessite les privilèges suivants : **Extension** > **Enregistrer une extension, Désenregistrer une extension, Mettre à jour une extension** Ce nouveau rôle doit être appliqué à l'objet vCenter dans la hiérarchie du serveur pour l'ID utilisateur spécifié lors de l'installation.
Serveur IBM Spectrum Protect **Restriction :** Le serveur doit être démarré.	Accès administrateur (Privilège **Système** ou **Domaine de règles non limité**)

Ports de communication requis

Affichez la liste des ports de communication devant être ouverts dans le pare-feu lors de l'installation de Data Protection for VMware.

Les ports identifiés dans le tableau correspondent à une installation typique. Une installation typique est constituée des composants suivants sur un même système Windows :

- Serveur de l'interface graphique de Data Protection for VMware
- Serveur de sauvegarde vStorage (dispositif de transfert de données)
- Proxy de montage Windows
- Interface de restauration de fichier de IBM Spectrum Protect

Si une installation non-typique est utilisée, davantage de ports peuvent être nécessaires.

Restriction : Le proxy de montage Windows et le proxy de montage Linux doivent se trouver sur le même sous-réseau.

Tableau 6. Ports de communication requis. Ce tableau identifie les ports auxquels Data Protection for VMware accède.

Port TCP	Initiateur : systèmes sortant (provenant de l'hôte)	Cible : système entrant (vers l'hôte)
443	Serveur de sauvegarde vStorage	Serveur vCenter (HTTP sécurisé)
443	Serveur de l'Interface graphique de Data Protection for VMware vSphere	Serveur vCenter
443 Ce paramètre est obligatoire uniquement lorsque le dispositif de transfert de données est un système Linux.	Proxy de montage Windows	Serveur vCenter
443	Serveur de sauvegarde vStorage	Platform Services Controller

Tableau 6. Ports de communication requis (suite). Ce tableau identifie les ports auxquels Data Protection for VMware accède.

Port TCP	Initiateur : systèmes sortant (provenant de l'hôte)	Cible : système entrant (vers l'hôte)
443	Serveur de l'Interface graphique de Data Protection for VMware vSphere	Platform Services Controller
443	Proxy de montage Windows	Platform Services Controller
902 443	Serveur vCenter	Hôtes ESXi
902 443	Serveur de sauvegarde vStorage (proxy)	Hôtes ESXi (tous les hôtes protégés)
1500 (**tcpport**)	Serveur de sauvegarde vStorage (proxy)	Serveur IBM Spectrum Protect
1500 (**tcpadminport**)	Serveur de l'Interface graphique de Data Protection for VMware vSphere • Le port 1500 (**tcpadminport**) prend en charge les communications non SSL. • Pour les communications SSL, **tcpadminport** est le seul port qui prend en charge les communications SSL avec le serveur IBM Spectrum Protect. Le numéro de port à utiliser pour le protocole SSL est généralement la valeur définie par l'option **ssltcpadminport** dans le fichier dsmserv.opt se trouvant sur le serveur IBM Spectrum Protect. Toutefois, si **adminonclient no** est spécifié dans le fichier dsmserv.opt, le numéro de port à utiliser pour le protocole SSL est la valeur définie par l'option **ssltcpadminport**. Aucune valeur par défaut n'est associée à l'option **ssltcpadminport**. Cette valeur doit donc être définie par l'utilisateur.	Serveur IBM Spectrum Protect
1527 Base de données Derby interne		
1501 1581 (**httpport**)	Serveur IBM Spectrum Protect	Serveur de sauvegarde vStorage • Planificateur de transfert de données • Client Web • Démon Client Acceptor
1581 (**httpport**) 1582, 1583 (**webports**)	Serveur de l'Interface graphique de Data Protection for VMware vSphere	Serveur de sauvegarde vStorage

Tableau 6. Ports de communication requis (suite). Ce tableau identifie les ports auxquels Data Protection for VMware accède.

Port TCP	Initiateur : systèmes sortant (provenant de l'hôte)	Cible : système entrant (vers l'hôte)
9081 Serveur Web de l'interface graphique (protocole HTTPS)	Client vSphere	Serveur de l'Interface graphique de Data Protection for VMware vSphere (port HTTPS sécurisé permettant d'accéder à vCenter via le navigateur Web)
22 Port SSH par défaut de l'agent de récupération	Recovery Agent	Hôte de "montage" Windows de Data Protection for VMware • SSH pour l'agent de récupération Linux
3260	Restauration de fichier Linux Data Protection for VMware	Hôte de "montage" Windows de Data Protection for VMware • iSCSI
3260 Port iSCSI par défaut de l'agent de récupération	Cible Windows avec disque dynamique pour restauration de fichier	Hôte de "montage" Windows de Data Protection for VMware • iSCSI
5985	Opérations de l'interface graphique de restauration de fichiers	Gestion à distance Windows
135	Proxy de montage Windows	Machine virtuelle VMware contenant les fichiers à restaurer avec l'interface de restauration de fichiers de IBM Spectrum Protect

Exigences en termes de privilèges utilisateur du serveur VMware vCenter

Des privilèges du serveur VMware vCenter sont nécessaires pour exécuter certaines opérations de Data Protection for VMware.

Privilèges du serveur vCenter requis pour protéger les centres de données VMware à l'aide de la vue du navigateur web pour l'Interface graphique de Data Protection for VMware vSphere

L'ID utilisateur du serveur vCenter utilisé pour la connexion à la vue du navigateur pour l'Interface graphique de Data Protection for VMware vSphere

doit avoir des privilèges VMware suffisants pour voir le contenu d'un centre de données géré par l'interface graphique.

Par exemple, un environnement VMware vSphere contient cinq centres de données. Un utilisateur, «jenn», possède des privilèges suffisants pour seulement deux de ces centres de données. En conséquence, seuls ces deux centres de données sont visibles par «jenn» dans les vues. Les trois autres centres de données (pour lesquels «jenn» ne possède pas de privilèges) ne sont pas visibles par l'utilisateur «jenn».

Le serveur VMware vCenter définit collectivement un ensemble de privilèges en tant que rôle. Un rôle s'applique à un objet pour un utilisateur ou un groupe spécifié pour créer un privilège. A partir du client Web VMware vSphere, vous devez créer un rôle avec un ensemble de privilèges. Pour créer un rôle de serveur vCenter pour des opérations de sauvegarde et de restauration, utilisez la fonction **Add a Role** du client WMware vSphere.

Si vous souhaitez propager les privilèges à tous les centres de données au sein de vCenter, spécifiez le serveur vCenter et cochez la case `Propagate to children`. Vous pouvez aussi limiter les droits si vous affectez le rôle aux centres de données requis uniquement à l'aide de la case à cocher `Propagate to children` sélectionnée. L'application pour l'interface graphique du navigateur s'effectue au niveau du centre de données.

L'exemple ci-après montre comment contrôler l'accès aux centres de données pour deux groupes d'utilisateurs VMware. Commencez par créer un rôle qui contient tous les privilèges définis dans la note technique 7047438. Les privilèges utilisés dans cet exemple sont identifiés par le rôle «TDPVMwareManage». Le groupe 1 nécessite un accès afin de restaurer des machines virtuelles pour les centres de données `Primary1_DC` et `Primary2_DC`. Le groupe 2 nécessite un accès afin de gérer des machines virtuelles pour les centres de données `Secondary1_DC` et `Secondary2_DC`.

Pour le groupe 1, affectez le rôle «TDPVMwareManage» aux centres de données `Primary1_DC` et `Primary2_DC`. Pour le groupe 2, affectez le rôle «TDPVMwareManage» aux centres de données `Secondary1_DC` et `Secondary2_DC`.

Les utilisateurs de chaque groupe d'utilisateurs VMware peuvent utiliser l'interface graphique de Data Protection for VMware pour gérer des machines virtuelles dans leurs centres de données respectifs uniquement.

Conseil : Lorsque vous créez un rôle, vous devez envisager de lui ajouter des privilèges supplémentaires dont vous aurez peut-être besoin pour effectuer d'autres tâches sur des objets.

Privilèges du serveur vCenter requis pour utiliser le dispositif de transfert de données

Le dispositif de transfert de données IBM Spectrum Protect qui est installé sur le serveur de stockage vStorage (noeud de dispositif de transfert de données) nécessite les options `VMCUser` et `VMCPw`. L'option `VMCUser` spécifie l'ID utilisateur du serveur vCenter ou ESX que vous souhaitez sauvegarder, restaurer ou interroger. Les privilèges requis affectés à cet ID utilisateur (`VMCUser`) garantissent que le client peut exécuter des opérations sur la machine virtuelle et dans l'environnement VMware. Cet ID utilisateur doit disposer des privilèges décrits dans la note technique ci-dessus.

Pour créer un rôle de serveur vCenter pour des opérations de sauvegarde et de restauration, utilisez la fonction **Add a Role** du client WMware vSphere. Vous devez sélectionner l'option `Propagate to children` lorsque vous ajoutez des privilèges pour cet ID utilisateur (`VMCUser`). De plus, vous devez envisager d'ajouter d'autres privilèges à ce rôle pour des tâches autres que la sauvegarde et la restauration. Pour l'option `VMCUser`, la mise en application s'effectue au niveau de l'objet sommet.

Privilèges du serveur vCenter requis pour protéger les centres de données VMware à l'aide de la vue du Plug-in client IBM Spectrum Protect vSphere pour l'Interface graphique de Data Protection for VMware vSphere

Le Plug-in client IBM Spectrum Protect vSphere nécessite un ensemble de privilèges distinct des privilèges qui sont nécessaires pour se connecter à l'interface graphique.

Lors de l'installation, les privilèges personnalisés suivants sont créés pour le Plug-in client IBM Spectrum Protect vSphere :

- **Centre de données** > **IBM Data Protection**
- **Global** > **Configuration d'IBM Data Protection**

Les privilèges personnalisés qui sont requis pour le Plug-in client IBM Spectrum Protect vSphere sont enregistrés en tant qu'extension distincte. La clé d'extension des privilèges est `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

Ces privilèges permettent à l'administrateur VMware d'activer et de désactiver l'accès au contenu du Plug-in client IBM Spectrum Protect vSphere. Seuls les utilisateurs dotés de ces privilèges personnalisés sur l'objet VMware requis peuvent accéder au contenu du Plug-in client IBM Spectrum Protect vSphere. Un Plug-in client IBM Spectrum Protect vSphere est enregistré pour chaque serveur vCenter et partagé par tous les hôtes d'interface graphique qui sont configurés pour prendre en charge le serveur vCenter.

A partir du client Web VMware vSphere, vous devez créer un rôle pour les utilisateurs qui peuvent exécuter des fonctions de protection des données des machines virtuelles à l'aide du Plug-in client IBM Spectrum Protect vSphere. Pour ce rôle, outre les privilèges de rôle administrateur de machine virtuelle standard requis par le client Web, vous devez spécifier le privilège **Centre de données** > **IBM Data Protection**. Pour chaque centre de données, affectez ce rôle à chaque utilisateur ou groupe d'utilisateurs auquel vous souhaitez accorder le droit de gérer des machines virtuelles.

Le privilège **Global** > **IBM Data Protection** est requis pour l'utilisateur au niveau de vCenter. Ce privilège permet à l'utilisateur de gérer, d'éditer ou de supprimer la connexion entre le serveur vCenter et le serveur Web de l'interface graphique de Data Protection for VMware vSphere. Affectez ce privilège aux administrateurs qui maîtrisent l'interface graphique de Data Protection for VMware vSphere qui protège leur serveur vCenter respectif. Gérez vos connexions au Plug-in client IBM Spectrum Protect vSphere sur la page Connections de l'extension.

L'exemple ci-après montre comment contrôler l'accès aux centres de données pour deux groupes d'utilisateurs. Le groupe 1 nécessite un accès afin de gérer des machines virtuelles pour les centres de données `NewYork _DC` et `Boston_DC`. Le groupe 2 nécessite un accès afin de gérer des machines virtuelles pour les centres de données `LosAngeles_DC` et `SanFranciso_DC`.

A partir du client VMware vSphere, créez par exemple le rôle «IBMDataProtectManage», affectez les privilèges de rôle administrateur de machine virtuelle standard, ainsi que le privilège **Datacenter** > **IBM Data Protection**.

Pour le groupe 1, affectez le rôle «IBMDataProtectManage» aux centres de données `NewYork _DC` et `Boston_DC`. Pour le groupe 2, affectez le rôle «IBMDataProtectManage» aux centres de données `LosAngeles_DC` et `SanFranciso_DC`.

Les utilisateurs de chaque groupe peuvent utiliser le Plug-in client IBM Spectrum Protect vSphere dans le client Web vSphere pour gérer des machines virtuelles dans leurs centres de données respectifs uniquement.

Problèmes liés à des droits insuffisants

Lorsque l'utilisateur du navigateur web ne dispose pas de droits suffisants pour un centre de données, l'accès à la vue est bloqué. Le message d'erreur GVM2013E est généré pour informer l'utilisateur qu'il ne dispose pas des droits suffisants pour accéder aux centres de données gérés. D'autres nouveaux messages sont également disponibles pour informer les utilisateurs des problèmes liés aux droits insuffisants. Pour résoudre les problèmes liés aux droits, vérifiez que le rôle utilisateur est bien configuré comme décrit dans les sections précédentes. Le rôle utilisateur doit disposer de tous les privilèges identifiés dans le tableau Privilèges requis pour l'ID utilisateur du serveur VCenter et le dispositif de transfert de données et ces privilèges doivent être appliqués au niveau du centre de données à l'aide de la case `propagate to children`.

Lorsque l'utilisateur du Plug-in client IBM Spectrum Protect vSphere ne dispose pas de droits suffisants pour accéder à un centre de données, les fonctions de protection des données du centre ainsi que son contenu ne sont pas accessibles à l'extension.

Lorsque l'ID utilisateur de IBM Spectrum Protect (spécifié par l'option `VMCUser`) ne dispose pas des droits suffisants pour une opération de sauvegarde et de restauration, le message suivant s'affiche :

```
ANS9365E Erreur d'interface de programme d'application VMware vStorage.
"Cette opération n'est pas autorisée."
```

Lorsque l'ID utilisateur de IBM Spectrum Protect ne dispose pas des droits suffisants pour afficher une machine, les messages suivants s'affichent :

```
Commande de sauvegarde de machine virtuelle lancée.
Nombre total de machines virtuelles à traiter : 1
ANS4155E Machine virtuelle 'tango' introuvable sur le serveur VMware.
ANS4148E La sauvegarde intégrale de la machine virtuelle 'foxtrot' a échoué
avec le code retour 4390
```

Pour plus d'informations sur l'utilisation des privilèges, voir la note **vCenter Server privileges required for the Data Protection for VMware vSphere GUI and data mover**.

Pour extraire des informations de journal via le serveur VMware Virtual Center pour plus d'informations sur les problèmes liés aux droits d'accès, procédez comme suit.

1. Dans vCenter Server Settings, sélectionnez **Logging Options** et affectez la valeur **Trivia (Trivia)** au paramètre **vCenter Logging**.
2. Recréez l'erreur liée aux droits d'accès.
3. Restaurez la valeur précédente du paramètre **vCenter Logging** pour éviter qu'un nombre excessif de données de journal ne soit collecté.

4. Dans System Logs, recherchez la chaîne `NoPermission` dans le journal de serveur vCenter le plus récent (`vpxd-wxyz.log`). Par exemple :

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
   vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Throw: vim.fault.NoPermission
   ```

   Ce message de journal indique que l'ID utilisateur ne possédait pas suffisamment de droits pour créer une image instantanée (`createSnapshot`).

Installation des composants de Data Protection for VMware

Vous pouvez installer certains ou la totalité des composants disponibles dans le module Data Protection for VMware correspondant à votre système d'exploitation.

Pourquoi et quand exécuter cette tâche

A l'aide du programme d'installation de Data Protection for VMware, vous pouvez installer les composants suivants :

- IBM Spectrum Protect Recovery Agent
- Windows Interface de ligne de commande de l'agent de récupération
- Windows Documentation (Fichier Readme et fichier de mentions légales)
- Fichier d'activation de Data Protection for VMware
- Interface graphique de Data Protection for VMware vSphere
- Dispositif de transfert de données, lequel inclut les éléments suivants :
  - Interface graphique
  - Client web
  - Fichiers d'exécution de l'API client (64 bits)
  - Ligne de commande du client d'administration
  - Fichiers d'exécution de l'API VMware vStorage

Vous pouvez choisir une installation complète ou utiliser l'option d'installation avancée option si vous souhaitez installer un dispositif de transfert de données (proxy de montage), un agent de récupération et les packages de support requis.

Conseil : Vous pouvez créer plusieurs dispositifs de transfert de données sur le même système que Data Protection for VMware ou sur des systèmes distants. Cette configuration permet d'augmenter les ressources disponibles pour leur utilisation par Data Protection for VMware. Les systèmes sur lesquels est installé le dispositif de transfert de données sont dénommés Serveurs de sauvegarde vStorage.

Obtention du package d'installation de Data Protection for VMware

Vous pouvez obtenir le package d'installation de Data Protection for VMware depuis un site de téléchargement IBM tel que IBM Passport Advantage.

Linux

Avant de commencer

Si vous comptez télécharger les fichiers, définissez la taille de fichier maximale de l'utilisateur système sur 'illimitée' pour vous assurer que les fichiers puissent être téléchargés correctement :

1. Pour vérifier la taille de fichier maximale, lancez la commande suivante :
   ```
   ulimit -Hf
   ```
2. Si la valeur 'illimitée' n'est pas affectée à la taille de fichier maximale de l'utilisateur système, changez-la en suivant les instructions de la documentation correspondant à votre système d'exploitation.

Procédure

1. Téléchargez le fichier du package approprié à partir de l'un des sites suivants :
   - Dans le cas d'une toute première installation ou d'une nouvelle édition, accédez à Passport Advantage à l'adresse suivante : http://www.ibm.com/software/lotus/passportadvantage/. Passport Advantage est l'unique site depuis lequel vous pouvez télécharger un fichier de package sous licence.
   - Pour consulter les informations les plus récentes, obtenir des mises à jour et des correctifs de maintenance, accédez au site du support IBM Spectrum Protect à l'adresse suivante : http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager.
2. Si vous avez téléchargé le package depuis un site de téléchargement IBM, procédez comme suit :
   a. Téléchargez le fichier du package dans le répertoire de votre choix. Le chemin ne doit pas comporter plus de 40 caractères. Prenez soin d'extraire les fichiers d'installation dans un répertoire vide. Ne les décompressez pas dans un répertoire contenant des fichiers extraits auparavant, ou d'autres fichiers.
   b. Linux Assurez-vous de disposer des droits d'exécution pour le package. Si nécessaire, modifiez les autorisations du fichier à l'aide de la commande suivante :
      ```
      chmod a+x nom_package.bin
      ```
   c. Linux Décompressez le package à l'aide de la commande suivante :
      ```
      ./nom_package.bin
      ```
      où *package_name* est le nom du fichier téléchargé.
   d. Windows Extrayez le package en cliquant deux fois sur *package_name*, où *package_name* est le nom du fichier téléchargé.

Installation des composants de Data Protection for VMware à l'aide de l'assistant d'installation

Vous pouvez installer les composants de Data Protection for VMware à l'aide de l'assistant d'installation.

Pourquoi et quand exécuter cette tâche

Windows Vous pouvez utiliser Suite Installer pour installer Data Protection for VMware et le dispositif de transfert de données.

Linux Vous pouvez utiliser le programme d'installation autonome pour installer Data Protection for VMware et le dispositif de transfert de données.

Installation des composants de Data Protection for VMware sur des systèmes Windows

Installation des composants et des fonctions de Data Protection for VMware à l'aide de l'assistant d'installation.

Avant de commencer

Avant d'installer les composants de Data Protection for VMware, vérifiez que les conditions suivantes sont réunies :

- Existence d'un ID utilisateur disposant d'un accès aux privilèges d'administrateur.
- Connectivité réseau à un serveur VMware vCenter Server 6.x (ou version ultérieure) avec accès aux privilèges d'administrateur.
- Connectivité réseau à un serveur IBM Spectrum Protect avec accès administrateur (privilèges **système** ou de **domaine de règles non limité**). Ce serveur doit être disponible et en cours d'exécution.
- Prenez soin de consulter les exigences suivantes :
  - «Configuration requise», à la page 13
  - «Droits d'installation requis», à la page 16
  - «Ports de communication requis», à la page 17

Avant d'installer Data Protection for VMware, vous devez prendre en compte les options suivantes :

Type d'installation

Installation standard
Sous une installation standard, tous les composants et fonctions de Data Protection for VMware sont installés.

Installation avancée
Le panneau d'installation avancée contient l'option permettant d'installer un dispositif de transfert de données individuel. Le processus installe alors un dispositif de transfert de données (proxy de montage), un agent de récupération et les packages de support requis sur le système. Utilisez cette option d'installation pour ajouter des dispositifs de transfert de données spécifiques. Cette option installe également des agents de protection d'application pour permettre la reprise de bases de données individuelles. Après l'installation, vous pouvez utiliser l'interface graphique de IBM Spectrum Protect pour configurer le dispositif de transfert de données et les services via un plug-in VMware vSphere.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'outil Suite Installer pour installer Data Protection for VMware. Le fichier `spinstall.exe` utilisé par l'outil Suite Installer est situé à la racine du package d'installation.

Pour consulter la liste des composants et des fonctions que vous pouvez installer, voir «Composants installables», à la page 1.

Procédure

Pour installer Data Protection for VMware, procédez comme suit depuis l'emplacement du fichier `spinstall.exe` du composant que vous désirez installer :

1. Cliquez deux fois sur le fichier `spinstall.exe`.
2. Suivez les instructions de l'assistant pour installer les composants sélectionnés.

Que faire ensuite

Pour accéder à l'Interface graphique de Data Protection for VMware vSphere, reportez-vous à la section suivante :

- «Accès à l'Interface graphique de Data Protection for VMware vSphere», à la page 32

L'assistant de configuration est automatiquement affiché la première fois que vous lancez l'interface graphique.

Installation de Data Protection for VMware sur des systèmes Linux

Installez Data Protection for VMware sur des systèmes Linux en utilisant le mode InstallAnywhere.

Avant de commencer

Avant d'installer Data Protection for VMware, vérifiez que les conditions suivantes sont réunies :

- Avant de continuer, vérifiez que l'ID utilisateur dispose du niveau d'autorisations requises et que les ports de communication requis sont ouverts.
- Le processus d'installation crée l'utilisateur `tdpvmware`. Vous devez exécuter toutes les commandes **`vmcli`** en tant qu'utilisateur `tdpvmware` et à l'aide de l'ID administrateur ou superutilisateur.
- Un serveur X Window est requis lors d'une installation en mode console.
- Prenez soin de consulter les exigences suivantes :
  - «Configuration requise», à la page 13
  - «Droits d'installation requis», à la page 16
  - «Ports de communication requis», à la page 17

Procédure

Pour installer Data Protection for VMware, procédez comme suit.

1. Depuis la racine du dossier d'installation, passez dans le répertoire `CD/Linux/DataProtectionForVMware`.
2. Depuis une ligne de commande, entrez la commande suivante :
   ```
   ./install-Linux.bin
   ```

Résultats

Si vous recevez des avertissements ou des erreurs, consultez les fichiers journaux pour plus d'informations. Voir «Activité de consignation au journal», à la page 88.

Si vous ne parvenez pas à installer Data Protection for VMware, reportez-vous à la procédure "Suppression manuelle de Data Protection for VMware" dans «Désinstallation de Data Protection for VMware sur un système Linux», à la page 38.

Exécution d'une installation propre de Data Protection for VMware sous Linux

Si une installation Linux est interrompue, vous pouvez généralement la redémarrer. Cependant, si l'installation ne se relance pas, une installation propre est requise.

Pourquoi et quand exécuter cette tâche

Avant de lancer une installation propre, vérifiez que le produit est supprimé. Effectuez les étapes suivantes pour vous assurer de disposer d'un environnement propre :

Procédure

1. Si l'Interface graphique de Data Protection for VMware vSphere est installée, procédez comme suit.
   a. Arrêtez l'Interface de ligne de commande Data Protection for VMware en exécutant cette commande :
   `/etc/init.d/vmcli stop`
   b. Arrêtez le serveur Web de l'Data Protection for VMware en exécutant cette commande :
   `/etc/init.d/webserver stop`
   c. Supprimez le module `.rpm` en exécutant cette commande :
   `rpm -e TIVsm-TDPVMwarePlugin`
2. Supprimez les entrées de produit du moteur de déploiement :
   a. Exécutez la commande suivante pour répertorier toutes les entrées du moteur de déploiement :
   `/usr/ibm/common/acsi/bin/de_lsrootiu.sh`
   b. Exécutez la commande suivante pour supprimer toutes les entrées du moteur de déploiement :
   `/usr/ibm/common/acsi/bin/deleteRootIU.sh <identificateur_unique_universel> <discriminant>`
   c. Supprimez le répertoire `/var/ibm/common`.
   d. Supprimez le répertoire `/usr/ibm/common`.
   e. Nettoyez le répertoire `/tmp` en supprimant le fichier `acu_de.log`, s'il existe.
   f. Supprimez le répertoire `/tmp` qui contient l'ID de l'utilisateur qui a installé le moteur de déploiement
   g. Supprimez toutes les entrées de moteur de déploiement du fichier système `/etc/inittab`. Les entrées son délimitées par `#Begin AC Solution Install block` et `#End AC Solution Install block`. Supprimez tout le texte entre ces délimiteurs et supprimez le texte de délimitation lui-même.
   h. Supprimez toutes les références au moteur de déploiement du fichier système `/etc/services`.
3. Supprimez tous les fichiers Data Protection for VMware de l'installation qui a échoué :
   a. Supprimez les fichiers du répertoire *<REP_INSTALL_UTILISATEUR>*, qui est le répertoire dans lequel la tentative d'installation ayant échoué a été effectuée. Par exemple : `/opt/tivoli/tsm/TDPVMware/`
   b. Supprimez les raccourcis du bureau.
4. Sauvegardez le fichier de registre global (`/var/.com.zerog.registry.xml`). Une fois ce fichier sauvegardé, supprimez toutes les balises faisant référence à Data Protection for VMware.

5. Supprimez les fichiers journaux situés sous le répertoire principal et contenant la chaîne `TDPVMware`. Par exemple : `IA-TDPVMware-00.log` ou `IA-TDPVMware_Uninstall-00.log`.
6. Supprimez l'utilisateur qui a exécuté l'Interface de ligne de commande Data Protection for VMware.
   a. Exécutez la commande suivante :
      ```
      userdel -r tdpvmware
      ```
   b. Exécutez la commande suivante :
      ```
      groupdel tdpvmware
      ```

      Conseil : Dans certaines versions de Linux, la commande **`userdel`** supprime également le groupe lorsqu'aucun autre utilisateur ne lui est associé. Par conséquent, ignorez les messages d'échec de commande.

Résultats

Une fois cette procédure terminée, lancez l'installation propre.

Installation des composants de Data Protection for VMware en mode silencieux

Vous pouvez installer Data Protection for VMware en arrière-plan. Au cours de cette installation silencieuse, aucun message ne s'affiche.

Pourquoi et quand exécuter cette tâche

Windows Vous pouvez utiliser Suite Installer pour installer Data Protection for VMware et le dispositif de transfert de données.

Linux Vous pouvez utiliser le programme d'installation autonome pour installer Data Protection for VMware et le dispositif de transfert de données.

Installation de Data Protection for VMware sur des systèmes Windows en mode silencieux

Installez tous les composants Data Protection for VMware et du dispositif de transfert de données en mode silencieux à l'aide de l'outil Suite Installer.

Avant de commencer

Avant d'installer Data Protection for VMware et le dispositif de transfert de données, vérifiez que votre système répond aux exigences énoncées dans les sections suivantes :

- «Configuration requise», à la page 13
- «Droits d'installation requis», à la page 16
- «Ports de communication requis», à la page 17

Pourquoi et quand exécuter cette tâche

Restriction : Toutes les fonctions sont installées dans leur emplacement par défaut. Pour localiser les répertoires d'installation par défaut des composants, consultez les sous-rubriques de la section «Composants installables», à la page 1.

Procédure

Pour installer Data Protection for VMware, procédez comme suit.

1. A partir d'une invite de commande, lancez la commande suivante :
   `cd dossier_extraction\TSMVMWARE_WIN`
2. Entrez la commande suivante :

   ```
   spinstall.exe /silent
   ```

   Le message suivant s'affiche lorsque vous montez un volume pour la première fois :

   ```
   Le pilote de volume virtuel n'est pas encore enregistré. Vous pouvez enregistrer
   l'agent de récupération
   du pilote maintenant. Lors de l'enregistrement, un
   avertissement contenant le logo Microsoft Windows peut apparaître.
   Acceptez cet avertissement afin de terminer l'enregistrement.
   Voulez-vous enregistrer le pilote de volume virtuel maintenant ?
   ```

   Pour continuer, entrez **Yes** afin d'enregistrer le pilote du volume virtuel.

Tâches associées:

«Désinstallation de Data Protection for VMware for Windows en mode silencieux», à la page 37

Installation en mode silencieux de Data Protection for VMware sur des systèmes Linux

Vous pouvez personnaliser les fonctions Data Protection for VMware à installer en mode silencieux sur un système d'exploitation Linux.

Avant de commencer

Avant d'installer Data Protection for VMware, vérifiez que les conditions suivantes sont réunies :

- Avant de continuer, vérifiez que l'ID utilisateur dispose du niveau d'autorisations requises et que les ports de communication requis sont ouverts.
- Le processus d'installation crée l'utilisateur `tdpvmware`. Vous devez exécuter toutes les commandes **`vmcli`** en tant qu'utilisateur `tdpvmware` et à l'aide de l'ID administrateur ou superutilisateur.
- Un serveur X Window est requis lors d'une installation en mode console.
- Prenez soin de consulter les exigences suivantes :
  - «Configuration requise», à la page 13
  - «Droits d'installation requis», à la page 16
  - «Ports de communication requis», à la page 17

Pourquoi et quand exécuter cette tâche

Data Protection for VMware propose les fonctions d'installation en mode silencieux suivantes pour les systèmes d'exploitation Linux :

Tableau 7. Fonctions de l'installation en mode silencieux de Data Protection for VMware

Fonction	Description	Installée par défaut ?
Documents	Fichier Readme	Oui

Tableau 7. Fonctions de l'installation en mode silencieux de Data Protection for VMware (suite)

Fonction	Description	Installée par défaut ?
TDPVMwareDM	L'installation de cette fonction inclut le fichier d'activation. Permet à IBM Spectrum Protect d'exécuter les types de sauvegarde suivants : • Sauvegarde de machine virtuelle incrémentielle périodique • Sauvegarde incrémentielle-permanente de machine virtuelle intégrale • Sauvegarde de machine virtuelle incrémentielle-permanente-incrémentielle Si vous déchargez des charges de travail de sauvegarde, ce fichier doit être installé sur le serveur de sauvegarde vStorage.	Oui
TDPVMwareGUI	Interface graphique de Data Protection for VMware vSphere. **Remarque :** Inclut également l'installation du fichier d'activation.	Non

Procédure

Pour installer Data Protection for VMware, effectuez les étapes suivantes à partir du répertoire où vous avez extrait les fichiers du package d'installation :

1. Ouvrez le fichier *chemin*`../Linux/DataProtectionForVMware/installer.properties` et supprimez la mise en commentaire de l'entrée suivante pour accepter la licence (*chemin* représentant ici le dossier d'installation) :

   ```
   LICENSE_ACCEPTED=TRUE
   ```

2. Choisissez l'une des méthodes suivantes pour installer les composants Data Protection for VMware :
   - Pour une installation par défaut, ouvrez le dossier `CD/Linux/DataProtectionForVMware` et entrez la commande suivante :

     ```
     ./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true
     ```

   - Pour une installation personnalisée, procédez comme suit :
     a. Modifiez le fichier `installer.properties` en lui ajoutant les valeurs appropriées :
        1) Spécifiez **`INSTALL_MODE=Custom`**. Prenez soin de supprimer le signe dièse (#) de cette instruction.
        2) Spécifiez les fonctions à installer avec l'option **`CHOSEN_INSTALL_FEATURE_LIST`**. Par exemple, toutes les fonctions sont installées avec la valeur suivante :

           ```
           CHOSEN_INSTALL_FEATURE_LIST=Docs,TDPVMwareDM,TDPVMwareGUI
           ```

     b. Depuis le dossier `CD/Linux/DataProtectionForVMware`, lancez la commande suivante :

        ```
        ./install-Linux.bin -i silent -f installer.properties
        ```

Premiers pas après l'installation de Data Protection for VMware

Après avoir installé Data Protection for VMware, préparez-vous à procéder à la configuration. L'utilisation de l'assistant de configuration constitue la méthode de prédilection pour configurer Data Protection for VMware.

Feuille de travail de configuration

Utilisez cette feuille de travail pour enregistrer des informations dont vous aurez besoin pour configurer et gérer Data Protection for VMware. La feuille de travail est destinée à vous aider à vous rappeler les valeurs que vous avez spécifiées après la configuration.

Tableau 8. Feuille de travail de configuration de Data Protection for VMware

Elément	Votre valeur	Remarques
Informations sur le serveur IBM Spectrum Protect		
Adresse du serveur IBM Spectrum Protect		
Port du serveur IBM Spectrum Protect		
ID/mot de passe de l'administrateur du serveur IBM Spectrum Protect		
Port d'administration du serveur IBM Spectrum Protect		
Options de définition de noeud		
Préfixe à ajouter aux noeuds		
Domaine de règles à utiliser lors de l'enregistrement de nouveaux noeuds		
Nom/mot de passe du noeud vCenter		
Nom/mot de passe du noeud VMCLI		
Noms/mots de passe des noeuds de centre de données **A faire :** Vous pouvez créer plusieurs noeuds de centre de données.		Le nom du noeud de centre de données est composé du préfixe spécifié, suivi par un trait de soulignement et du nom du centre de données. Par exemple : *préfixeNoeud_nomCentreDonnées*
Noms/mots de passe de noeuds de dispositif de transfert de données sur le serveur de sauvegarde vStorage **A faire :** Vous pouvez créer plusieurs noeuds de dispositif de transfert de données.		Le nom du noeud de dispositif de transfert de données est composé du nom de noeud du centre de données, suivi d'un trait de soulignement et de DM. Par exemple : *nomNoeudCentreDonnées*_DM
Noms/mots de passe de noeuds de dispositif de transfert de données sur les serveurs distants **A faire :** Vous pouvez créer plusieurs noeuds de dispositif de transfert de données qui ne résident pas sur le serveur de sauvegarde vStorage.		
Noeud proxy de montage Le noeud proxy de montage est utilisé lorsque vous restaurez des données.	Windows: Linux:	

Tableau 8. Feuille de travail de configuration de Data Protection for VMware (suite)

Elément	Votre valeur	Remarques

Accès à l'Interface graphique de Data Protection for VMware vSphere

Utilisez l'Interface graphique de Data Protection for VMware vSphere pour créer une sauvegarde, restaurer et gérer des machines virtuelles dans un environnement VMware vCenter.

Avant de commencer

Pour pouvoir accéder à l'Interface graphique de Data Protection for VMware vSphere, vous devez avoir sélectionné lors de l'installation l'option de protection de vos données dans un environnement vSphere.

Procédure

- Si vous avez sélectionné l'option **Activer l'accès à l'interface graphique via un navigateur Web** lors de l'installation, vous pouvez accéder à l'Interface graphique de Data Protection for VMware vSphere depuis le navigateur :
  1. Ouvrez un navigateur Web et entrez l'URL suivante :

     `https://`*`nom_hôte`*`:`*`port`*`/TsmVMwareUI`

     où :
     - *nom_hôte* désigne le nom du système sur lequel l'Interface graphique de Data Protection for VMware vSphere est installée.
     - *port* désigne le numéro du port à travers lequel l'interface graphique de vSphere est accessible. Par défaut, il s'agit du port 9081.
  2. Connectez-vous avec votre ID utilisateur et mot de passe vCenter.
- Si vous n'avez pas sélectionné l'option **Activer l'accès à l'interface graphique via un navigateur Web** lors de l'installation, vous pouvez lancer l'Interface graphique de Data Protection for VMware vSphere en procédant comme suit :
  1. Ouvrez le client VMware vSphere et connectez-vous avec l'ID utilisateur et le mot de passe vCenter.
  2. Dans le panneau Solutions et applications du client vSphere, cliquez sur l'icône de l'Interface graphique de Data Protection for VMware vSphere.

Mise à niveau de Data Protection for VMware

Vous pouvez mettre à niveau Data Protection for VMware à partir d'une de ses versions précédentes.

Pour connaître la compatibilité avec les versions antérieures, voir la note technique 1993819.

Mise à niveau vers la version 7.1.8 : Si un message s'affiche lors de la procédure de mise à niveau pour vous inviter à remplacer le fichier `jextract` existant, sélectionnez **Oui pour tout**.

Mise à niveau de Data Protection for VMware

Cette procédure documente la mise à niveau vers Data Protection for VMware V8.1.4.

Avant de commencer

Important : Cette procédure de mise à niveau s'applique aux systèmes sur lesquels IBM Spectrum Protect Snapshot for VMware n'est pas installé.

Vous devez disposer des privilèges d'administrateur pour mettre à niveau Data Protection for VMware.

Les mises à jour vers l'Interface graphique de Data Protection for VMware vSphere existante sont traitées de la façon suivante :

- Les fichiers de paramètres sont sauvegardés avant le début de la procédure de mise à niveau de l'Interface graphique de Data Protection for VMware vSphere.
- Les mêmes numéros de port de base par défaut sont utilisés pour la base de donnés Derby et WebSphere Application Server.
- Linux Les valeurs indiquées dans le profil (`vmcliprofile`) sont utilisées pour l'Interface de ligne de commande Data Protection for VMware.

Restriction :

- Windows Lorsque IBM Spectrum Protect for Virtual Environments a été installé ailleurs qu'à l'emplacement par défaut, le processus de mise à niveau installe les fonctions de IBM Spectrum Protect for Virtual Environments V8.1.4 sous le répertoire d'installation par défaut. La mise à niveau ne doit pas être effectuée dans un emplacement autre que l'emplacement par défaut. Reportez-vous aux sous-rubriques dans «Composants installables», à la page 1 pour identifier le répertoire d'installation par défaut de chaque fonction.
- Linux Windows Le processus de mise à niveau n'installe pas de nouveau composant.

  Par exemple, si seule l'interface graphique Recovery Agent est installée sur la version précédente, la procédure de mise à niveau n'installe pas l'interface de ligne de commande Recovery Agent. Dans un tel scénario, vous devez réexécuter le programme d'installation puis sélectionner le composant manquant à installer.
- Linux La version de Recovery Agent sur Linux doit être identique à la version de Recovery Agent installée sur le proxy Windows. Si vous mettez à niveau Recovery Agent sous Linux, vous devez donc également mettre à niveau la version de Recovery Agent installée sur le proxy Windows.

Procédure

Pour mettre à niveau Data Protection for VMware, procédez comme suit.

1. Arrêtez les composants et les services Data Protection for VMware en cours d'exécution.
2. Démontez tous les volumes virtuels montés. Vous pouvez utiliser l'interface graphique de Recovery Agent ou l'interface de ligne de commande (commande **`mount del`**) pour démonter des volumes.
3. Suivez les instructions de la section «Installation des composants de Data Protection for VMware sur des systèmes Windows», à la page 25.

Remarque : Linux Si le dispositif de transfert de données version 6.x est installé, vous devez le désinstaller avant d'installer la V8.1.4. Suivez les instructions de la rubrique Désinstallation du client IBM Spectrum Protect Linux x86_64.

4. Téléchargez le package de code.
5. Depuis le dossier où vous avez sauvegardé le module de code, lancez le processus de mise à niveau :

   a. Windows Exécutez le fichier `spinstall.exe`.

   b. Linux Exécutez le fichier `install-Linux.bin`.

   Vous ne pouvez installer qu'une seule Interface graphique de Data Protection for VMware vSphere sur une machine. Il en résulte que plusieurs interfaces graphiques de Data Protection for VMware vSphere ne sont pas autorisées sur la même machine.

Mise à niveau de Data Protection for VMware sur un système Windows 64 bits en mode silencieux

Vous pouvez mettre à niveau Data Protection for VMware en mode silencieux sur un système d'exploitation 64 bits pris en charge.

Avant de commencer

Lorsque Data Protection for VMware version 6.x a été installé dans un emplacement autre que l'emplacement par défaut, la procédure de mise à niveau en mode silencieux installe les fonctions Data Protection for VMware V8.1.4 dans le répertoire d'installation par défaut. La mise à niveau en mode silencieux ne doit pas être effectuée dans un emplacement autre que l'emplacement par défaut. Reportez-vous aux sous-rubriques dans «Composants installables», à la page 1 pour identifier le répertoire d'installation par défaut de chaque fonction.

Procédure

Pour mettre à niveau Data Protection for VMware, procédez comme suit.

1. Arrêtez les composants Data Protection for VMware en cours d'exécution.
2. Démontez tous les volumes virtuels montés. Vous pouvez utiliser l'interface graphique de Recovery Agent ou l'interface de ligne de commande (commande **`mount del`**) pour démonter des volumes.
3. Démontez tous les volumes virtuels montés. Vous pouvez utiliser l'interface graphique de Recovery Agent ou l'interface de ligne de commande (commande **`mount del`**) pour démonter des volumes.
4. Téléchargez le package de code.
5. Dans le dossier de Data Protection for VMware, vous pouvez accéder au dossier X64.
6. Dans la fenêtre d'invite de commande, entrez la commande suivante :

   ```
   spinstall.exe /s /v"/qn REBOOT=ReallySuppress"
   ```

Mise à niveau de Data Protection for VMware sur un système Linux en mode silencieux

Vous pouvez mettre à niveau Data Protection for VMware sur un système d'exploitation Linux pris en charge.

Pourquoi et quand exécuter cette tâche

Utilisez les paramètres Data Protection for VMware suivants avec la fonction d'installation en mode silencieux :

Tableau 9. Paramètres de mise à niveau de l'installation en mode silencieux de Data Protection for VMware

Paramètre	Description	Valeur par défaut
VCENTER_HOSTNAME	Nom de domaine complet ou adresse IP du serveur vCenter.	Néant
VCENTER_USERNAME	ID utilisateur vCenter. Cet ID doit correspondre à un administrateur VMware disposant des droits nécessaires pour enregistrer des extensions et en annuler l'enregistrement.	Néant
VCENTER_PASSWORD	Mot de passe vCenter.	Néant
DIRECT_START	Pour accéder à l'Interface graphique de Data Protection for VMware vSphere dans un navigateur Web, spécifiez **DIRECT_START=YES**. Vous pouvez accéder à l'Interface graphique de Data Protection for VMware vSphere via un signet d'URL pointant sur le serveur Web de l'interface graphique. Si vous ne souhaitez pas accéder à l'Interface graphique de Data Protection for VMware vSphere dans un navigateur Web, spécifiez **DIRECT_START=NO**.	YES **Important :** Une fois la mise à niveau terminée, il est impossible de changer la valeur de **DIRECT_START**, sauf en réinstallant le produit.

Procédure

Pour mettre à niveau Data Protection for VMware, procédez comme suit.

1. Assurez-vous qu'il n'existe pas de session active de sauvegarde, de restauration ou de montage.
2. Vérifiez que chaque Interface graphique de Data Protection for VMware vSphere ou interface graphique de Recovery Agent existante est fermée.
3. Téléchargez le package de code.
4. Depuis le dossier Data Protection for VMware, accédez au dossier Linux.
5. Dans une fenêtre d'invite de commande, entrez la commande `././install-Linux.bin -i silent -DLICENSE_ACCEPTED=true` avec les paramètres préférés.
   Par exemple :

```
././install-Linux.bin -i silent -LICENSE_ACCEPTED=true
-VCENTER_HOSTNAME=hostname -VCENTER_USERNAME=username
-VCENTER_PASSWORD=password
-DIRECT_START=yes -REGISTER_PLUGIN=yes
```

Désinstallation de Data Protection for VMware

Le processus de désinstallation de Data Protection for VMware est le même pour une nouvelle installation et pour une version mise à niveau.

Désinstallation de Data Protection for VMware sous Windows

Désinstallation de composants Data Protection for VMware et suppression des fichiers et répertoires d'un système Windows.

Avant de commencer

Pour garantir la réussite de la désinstallation, prenez en compte les éléments suivants :

- Si d'autres hôtes d'interface graphique Web de Data Protection for VMware utilisent le Plug-in client IBM Spectrum Protect vSphere, n'annulez pas l'enregistrement de l'extension client Web.

Pourquoi et quand exécuter cette tâche

Les fichiers de configuration et de propriété se trouvent dans le répertoire `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config` une fois la désinstallation terminée.

Procédure

1. Arrêtez les composants Data Protection for VMware en cours d'exécution.
2. Démontez tous les volumes virtuels montés.
3. Supprimez les éventuelles sauvegardes existantes de machine virtuelle à l'aide de la commande `delete backup` du dispositif de transfert de données.
4. Supprimez les services de dispositif de transfert de données installés à l'aide de la commande `dsmcutil remove`.

   Pour obtenir la liste des services, accédez à `C:\Program Files\Tivoli\TSM\baclient\` et exécutez la commande `dsmcutil list`.

   Supprimez les services à l'aide de commandes similaires aux commandes suivantes, en adaptant le nom figurant entre guillemets pour indiquer le service :

   ```
   dsmcutil remove /name:"TSM Remote Client Agent"
   dsmcutil remove /name:"TSM Client Acceptor"
   ```
5. Cliquez sur **Démarrer** > **Panneau de configuration** > **Programmes et fonctions** > **Désinstaller un programme**. Désinstallez les programmes suivants :
   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware Suite
   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware License
   - IBM Spectrum Protect: JVM
6. Supprimez les fichiers et répertoires Data Protection for VMware suivants du système de fichiers, le cas échéant. Pour IBM Spectrum Protect for Virtual Environments versions 8.1.6 et ultérieures, supprimez :

   ```
   C:\IBM\SpectrumProtect
   C:\Program Files\IBM\SpectrumProtect
   C:\ProgramData\Tivoli\TSM
   C:\ProgramData\config
   C:\IBM\SpectrumProtect
   C:\Program Files\IBM\SpectrumProtect
   ```

Vous pouvez également supprimer :

```
C:\Program Files\Tivoli\TSM
```

si les fichiers journaux et les fichiers de configuration sont devenus inutiles. Si vous souhaitez conserver ces fichiers, ils se trouvent dans `C:\Program Files\Tivoli\TSM\baclient`. Pour IBM Spectrum Protect for Virtual Environments versions 8.1.4 et antérieures, supprimez :

```
C:\IBM\tivoli
C:\Program Files (x86)\Common Files\Tivoli\TDPVMware
C:\Program Files\Common Files\Tivoli
C:\ProgramData\Tivoli\TSM
C:\ProgramData\config
```

Vous pouvez également supprimer :

```
C:\Program Files\Tivoli\TSM
```

si les fichiers journaux et les fichiers de configuration sont devenus inutiles. Si vous souhaitez conserver ces fichiers, ils se trouvent dans `C:\Program Files\Tivoli\TSM\baclient`.

Que faire ensuite

Vérifiez que tous les composants ont été retirés du système.

Désinstallation de Data Protection for VMware for Windows en mode silencieux

Vous pouvez désinstaller Data Protection for VMware en mode silencieux sur un système d'exploitation Windows.

Pourquoi et quand exécuter cette tâche

Les fichiers de configuration et de propriété se trouvent dans le répertoire `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config` une fois la désinstallation terminée.

Procédure

Pour désinstaller Data Protection for VMware, procédez comme suit.

1. Arrêtez les composants Data Protection for VMware en cours d'exécution.
2. Démontez tous les volumes virtuels montés. Vous pouvez utiliser l'interface graphique de Recovery Agent ou l'interface de ligne de commande (commande **mount del**) pour démonter des volumes.
3. Dans une fenêtre d'invite de commande, utilisez la commande **cd** pour accéder à l'un des dossiers suivants :
   - Pour personnaliser l'opération de désinstallation, accédez au dossier `X64`.
   - Pour désinstaller Data Protection for VMware à l'aide de l'outil Suite Installer, accédez à `<dossier d'extraction>TSM4VE_WIN` :
4. Dans la fenêtre d'invite de commande, exécutez la commande suivante :
   - Pour une opération de désinstallation personnalisée, sélectionnez l'une des commandes suivantes :
     – Pour désinstaller Data Protection for VMware et annuler l'enregistrement de l'Interface graphique de Data Protection for VMware vSphere, entrez la commande suivante :

```
spinstall.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
VCENTER_HOSTNAME=<nom d'hôte ou IP vCenter>
VCENTER_USERNAME=<nom d'utilisateur vCenter>
VCENTER_PASSWORD=<mot de passe vCenter>"
```

- Pour désinstaller toutes les fonctions à l'aide du programme d'installation Suite, entrez la commande suivante :

  ```
  spinstall.exe /silent /remove
  ```

5. Une fois la désinstallation terminée, redémarrez le système.

Désinstallation de Data Protection for VMware sur un système Linux

Désinstallez Data Protection for VMware et supprimez les fichiers et répertoires d'un système d'exploitation Linux.

Avant de commencer

Pour garantir la réussite de la désinstallation, prenez en compte les éléments suivants :

- Retirez les noeuds d'IBM Spectrum Protect Server. Vous devez effectuer cette opération avant de désinstaller le produit Data Protection for VMware :
  1. Exécutez `dsmadmc` depuis `/opt/tivoli/tsm/client/ba/bin/dsmadmc`.
  2. Il se peut que vous deviez utiliser la commande `del` pour supprimer l'espace fichier des noeuds : `del file` *`nom_noeud`* `*`
  3. Utilisez la commande `q` pour interroger les noeuds : `q filespace` *`nom_noeud`* `*`
  4. Utilisez la commande `rem` pour retirer les noeuds : `rem node` *`nom_noeud`*
- Arrêtez les services `dsmcad` créés pour les dispositifs de transfert de données. Utilisez les instructions figurant dans la note technique http://www-01.ibm.com/support/docview.wss?uid=swg21358414
  1. Utilisez la commande `ps` pour vérifier si le service `dsmcad` est en cours d'exécution : `ps -ef|grep dsmcad`
  2. Utilisez la commande `kill` pour arrêter le service `dsmcad` : `kill -9` *`ID_processus_dsmcad`*
- Vous devez nettoyer les fichiers liés à la création des services de dispositif de transfert de données. Accédez au répertoire d'installation et lancez la commande suivante :

  ```
  /opt/tivoli/tsm/client/ba/bin/dsmutillnx cleanupDmFiles 1
  ```

  Appuyez sur Entrée pour sélectionner le nom du noeud, puis appuyez sur Entrée pour le supprimer.

  Vous trouverez les noms de noeud dans `dsm.sys`.
- Lorsque vous désinstallez le Plug-in client IBM Spectrum Protect vSphere d'un environnement VMware vSphere 5.5, seuls les intitulés et les descriptions de privilège qui lui sont associés sont retirés. Les privilèges réels restent installés. Ce problème est une limitation VMware connue. Pour plus d'informations, voir l'article suivant dans la base de connaissances VMware : http://kb.vmware.com/kb/2004601.
- Le fichier d'activation de Data Protection for VMware n'est pas supprimé après la désinstallation du produit.

Pourquoi et quand exécuter cette tâche

Lorsque vous désinstallez Data Protection for VMware sur un système Linux, le type de désinstallation est par défaut identique à celui de l'installation d'origine. Pour utiliser un processus d'installation différent, spécifiez le paramètre correct. Par exemple, si vous avez utilisé un processus d'installation en mode silencieux, vous pouvez utiliser l'assistant d'installation pour la désinstallation en spécifiant le paramètre `–i swing`. Exécutez le processus de désinstallation en tant que superutilisateur. Le profil de superutilisateur doit être sourcé. Si vous utilisez la commande `su` pour basculer en superutilisateur, utilisez la commande `su -` pour sourcer le profil de superutilisateur.

Lorsque le processus de désinstallation commence à supprimer les fichiers du programme, annuler le processus de désinstallation ne ramène pas le système à un état propre. Cette situation peut entraîner l'échec de la tentative de réinstallation. Par conséquent, nettoyez le système en effectuant les tâches décrites dans «Suppression manuelle de Data Protection for VMware d'un système Linux», à la page 40.

Pour désinstaller Data Protection for VMware, procédez comme suit :

Procédure

1. Sélectionnez le répertoire du programme de désinstallation. Le chemin suivant est l'emplacement par défaut du programme de désinstallation : `/opt/tivoli/tsm/tdpvmware/_uninst/TDPVMware/`
2. Selon le type d'installation, utilisez l'une des méthodes suivantes pour désinstaller Data Protection for VMware :

   Remarque : Les commandes de cette procédure doivent être entrées sur une seule ligne. Ces exemples présentent deux lignes pour des raisons de mise en page.

   - Pour utiliser l'assistant d'installation afin de désinstaller Data Protection for VMware, entrez la commande suivante :

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware –i swing
     ```

   - Pour utiliser la console afin de désinstaller Data Protection for VMware, entrez la commande suivante :

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware -i console
     ```

   - Pour désinstaller Data Protection for VMware en mode silencieux, entrez la commande suivante :

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware -i silent
     -f uninstall.properties
     ```

     Le fichier `uninstall.properties` contient les informations de connexion de vCenter. Ces informations sont nécessaires à la désinstallation de l'Interface graphique de Data Protection for VMware vSphere.

Suppression manuelle de Data Protection for VMware d'un système Linux

Pourquoi et quand exécuter cette tâche

Lorsqu'il est impossible de désinstaller Data Protection for VMware à l'aide de la procédure de désinstallation standard, vous devez supprimer manuellement Data Protection for VMware du système en procédant comme suit. Exécutez ce processus en tant que superutilisateur.

Procédure

1. Si vous avez installé l'Interface graphique de Data Protection for VMware vSphere, supprimez son package de la base de données du gestionnaire de packages (Package Manager) à l'aide de la commande suivante :

   ```
   rpm -e TIVsm-TDPVMwarePlugin
   ```

2. Supprimez l'API IBM Spectrum Protect à l'aide de la commande suivante :

   ```
   rpm -e TIVsm-API64
   gskssl64.linux.x86_64.rpm
   skcrypt64.linux.x86_64
   TIVsm-TDPVMwarePlugin.x86_64.rpm
   TIVsm-DPAPI.x86_64.rpm
   ```

3. Supprimez les entrées de produit du moteur de déploiement :
   a. Exécutez cette commande pour afficher une liste de toutes les entrées :

      ```
      /usr/ibm/common/acsi/bin/de_lsrootiu.sh
      ```

   b. Exécutez cette commande pour supprimer les entrées d'unité installées associées à Data Protection for VMware :

      ```
      /usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <discriminant>
      ```

      Assurez-vous que ces entrées d'unité sont supprimées :

      ```
      FBJRE
      TDPVMwareGUI
      JavaHelp
      TDPVMwareDM
      ```

      Une fois le programme de désinstallation terminé, supprimez les répertoires suivants, le cas échéant :

      - `/opt/tivoli/tsm/client`
      - `/opt/tivoli/tsm/tdpvmware`

      Supprimez l'utilisateur `tdpvmware` et les répertoires associés :

      - `userdel tdpvmware`
      - `/home/tdpvmware`
      - `/etc/adsm`

4. Sauvegardez le fichier de registre global (`/var/.com.zerog.registry.xml`). Une fois le fichier sauvegardé, supprimez toutes les balises associées à Data Protection for VMware.
5. Supprimez tous les fichiers du répertoire d'installation (`/opt/tivoli/tsm/tdpvmware`). Supprimez également tous les raccourcis présents sur le bureau.
6. Sauvegardez les fichiers journaux situés dans le répertoire `/root` et dont le nom contient `TDPVMware`. Par exemple, `IA-TDPVMware-00.log` ou `IA-TDPVMware_Uninstall-00.log`. Supprimez ces fichiers journaux une fois qu'ils sont sauvegardés. En les supprimant, vous pouvez afficher les erreurs renvoyées si le processus d'installation échoue à nouveau.

7. Vous pouvez maintenant installer à nouveau le produit, comme indiqué dans «Installation de Data Protection for VMware sur des systèmes Linux», à la page 26.

Modification d'une installation existante de Data Protection for VMware

La présente section fournit des instructions pour modifier les fonctions et packages d'une installation existante de Data Protection for VMware.

A l'aide du programme d'installation Suite Installer, vous pouvez changer quels packages sous-jacents sont installés sur le système. Pour modifier les fonctions d'un package spécifique, vous pouvez utiliser la section **Programmes et fonctionnalités** du Panneau de configuration de Windows.

Modification des packages dans une installation existante de Data Protection for VMware

Vous pouvez utiliser le programme d'installation Suite Installer pour changer les packages d'une installation existante de Data Protection for VMware.

Avant de commencer

Veillez à disposer du support source avant d'utiliser le programme d'installation Suite Installer. Le fichier exécutable `spinstall.exe` du programme d'installation Suite Installer se trouve à la racine du package d'installation.

Pourquoi et quand exécuter cette tâche

Utilisez le programme d'installation Suite Installer pour modifier les packages installés dans une installation existante de Data Protection for VMware. Vous pouvez choisir d'ajouter ou de supprimer :

- Le dispositif de transfert de données
- Data Protection for VMware

Procédez comme suit :

Procédure

1. Cliquez deux fois sur le fichier `spinstall.exe` pour exécuter le package du programme d'installation Suite Installer.
2. Utilisez les cases à cocher du panneau **Installation personnalisée** pour déterminer les packages que vous avez besoin d'installer.
3. Sélectionnez les packages requis pour cette installation.

Modification de fonctions dans une installation existante de Data Protection for VMware

Vous pouvez utiliser la section Programmes et fonctionnalités du Panneau de configuration de Windows pour changer les fonctions d'une installation existante de Data Protection for VMware.

Avant de commencer

Veillez à disposer du support source avant de modifier le package d'installation.

Pourquoi et quand exécuter cette tâche

Utilisez Windows pour modifier les fonctions individuelles étant disponibles dans une installation existante de Data Protection for VMware. Vous pouvez choisir de modifier les fonctions :

- Du dispositif de transfert de données
- Data Protection for VMware

Procédez comme suit :

Procédure

1. Dans la section **Programmes et fonctionnalités** du **Panneau de configuration** de Windows, cliquez à l'aide du bouton droit de la souris sur l'application IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.
2. Cliquez sur **Modifier** pour mettre à jour les fonctions du package actuellement installées.
3. Sélectionnez les fonctions requises pour cette installation.

Chapitre 2. Configuration de Data Protection for VMware

Cette section contient des instructions relatives à la configuration de Data Protection for VMware et au démarrage des services associés.

Configuration d'une nouvelle installation à l'aide de l'assistant

Utilisez l'assistant de configuration pour la configuration initiale ou pour apporter des modifications mineures.

Avant de commencer

Le système sur lequel Data Protection for VMware est installé doit disposer d'une connectivité réseau aux serveurs suivants :

- Serveur de sauvegarde vStorage
- Serveur IBM Spectrum Protect
- Serveur vCenter

Pourquoi et quand exécuter cette tâche

Pour configurer l'environnement Data Protection for VMware, procédez comme suit :

Procédure

1. Ouvrez un navigateur Web et entrez l'adresse du serveur Web de l'interface graphique. Par exemple :

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

   - Dans un environnement vSphere, connectez-vous avec le nom d'utilisateur et le mot de passe vCenter.
2. Dans la fenêtre Initiation, accédez à la fenêtre Configuration et cliquez sur **Lancer l'assistant de configuration**.
3. Suivez les instructions contenues dans chaque page de l'assistant, jusqu'à ce que la fenêtre Récapitulatif s'affiche. Vérifiez les paramètres et cliquez sur **Terminer** pour terminer la configuration et quitter l'assistant.

   Conseil : L'aide en ligne installée avec l'interface graphique contient des informations sur chaque page de configuration. Cliquez sur **En savoir plus** dans l'une des fenêtres de l'interface pour ouvrir l'aide en ligne et obtenir de l'assistance. Consultez la rubrique *Exécution de l'assistant de configuration*.
4. Vérifiez que les noeuds de dispositif de transfert de données sont configurés correctement :
   a. Cliquez sur l'onglet **Configuration** pour afficher la page Etat de la configuration.
   b. Dans la page Etat de la configuration, sélectionnez un noeud de dispositif de transfert de données pour afficher ses informations de statut dans le panneau Détails de l'état. Lorsqu'un noeud affiche un avertissement ou une erreur, cliquez sur ce noeud et utilisez les informations du panneau Détails du statut pour résoudre l'incident. Puis, sélectionnez le noeud et cliquez sur **Valider le noeud sélectionné** pour vérifier si l'anomalie est résolue. Cliquez sur **Actualiser** pour retester tous les noeuds.

Résultats

Raccourci : Une fois la tâche d'assistant correctement exécutée, aucune tâche de configuration supplémentaire n'est requise pour la sauvegarde des données de machine virtuelle.

Utilisation du bloc-notes pour modifier une installation existante

Utilisez le bloc-notes d'édition de la configuration pour éditer les paramètres de configuration existants.

Avant de commencer

Le bloc-notes d'édition de la configuration propose les tâches relatives à la configuration existante suivantes :

- Définir ou modifier l'ID administrateur IBM Spectrum Protect.
- Réinitialisez le mot de passe et déverrouillez le mode VMCLI.
- (Environnement vSphere) Ajout ou suppression de centres de données VMware au domaine de votre Interface graphique de Data Protection for VMware vSphere.
- Ajout ou suppression de noeuds proxy de montage. Modification du mot de passe d'un noeud proxy de montage existant.
- Ajout ou suppression de noeuds de dispositif de transfert de données. Modification du mot de passe d'un noeud de dispositif de transfert de données existant.
- Activation de la restauration de fichier.
- Activation de la prise en charge du balisage pour un noeud de dispositif de transfert de données.

Pourquoi et quand exécuter cette tâche

Pour éditer une configuration existante, procédez comme suit.

Procédure

1. Ouvrez un navigateur Web et entrez l'adresse du serveur Web de l'interface graphique. Par exemple :

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

   Connectez-vous avec le nom d'utilisateur et le mot de passe vCenter.
2. Dans la fenêtre Initiation, accédez à la fenêtre Configuration et cliquez sur **Modifier la configuration**.
3. Accédez à la page correspondant à votre tâche d'édition et suivez les instructions. Vous devez cliquer sur **OK** pour sauvegarder vos modifications avant de passer à une autre page des paramètres de configuration. Sinon, vos modifications ne seront pas prises en compte.

   Important : L'aide en ligne installée avec l'interface graphique contient des informations sur chaque page de configuration. Cliquez sur **En savoir plus** dans l'une des fenêtres de l'interface pour ouvrir l'aide en ligne et obtenir de l'assistance. Consultez la rubrique *Edition d'une configuration existante*.

Résultats

Les paramètres mis à jour s'affichent dans la fenêtre Configuration.

Activation de l'environnement pour les opérations de restauration de fichier

Windows

Lorsque la fonction de restauration de fichier est activée par un administrateur, les propriétaires de fichier peuvent restaurer des fichiers sans l'aide de l'administrateur.

Avant de commencer

Si vous n'avez pas vérifié que tous les prérequis sont respectés, consultez la rubrique consacrée aux prérequis pour la restauration de fichiers dans le *Guide d'utilisation d'IBM Spectrum Protect for Virtual Environments : Data Protection for VMware*.

Pourquoi et quand exécuter cette tâche

Procédez comme suit sur le système où l'Interface graphique de Data Protection for VMware vSphere est installée.

Procédure

1. Lancez l'Interface graphique de Data Protection for VMware vSphere en ouvrant un navigateur Web et en entrant l'adresse du serveur Web de l'interface graphique. Par exemple :

   `https://<adresse_serveur_web_interface_graphique>:9081/TsmVMwareUI/`

   Connectez-vous avec l'ID utilisateur et le mot de passe vCenter.
2. Dans la fenêtre Initiation, cliquez sur **Configuration** et sélectionnez l'une des tâches suivantes dans la liste Tâches :
   - Si vous configurez un nouvel environnement, procédez comme suit :
     a. Sélectionnez **Lancer l'assistant de configuration du client**.
     b. Suivez les instructions contenues dans chaque page de l'assistant. Suivez les indications ci-après pour renseigner la page Restauration de fichier :
        1) Sélectionnez l'option **Activer la restauration de fichier**.
        2) Entrez les informations de contact administrateur affichées dans l'interface de restauration de fichier. Si vous ne voulez pas fournir d'informations de contact, désélectionnez la case à cocher.
        3) Si l'environnement contient des sauvegardes de machines virtuelles Windows, entrez les données d'identification de l'administrateur du domaine Windows. Sinon, ne cochez pas la case et n'entrez pas de données d'identification.

           Conseil : Une opération de restauration de fichier utilise les données d'identification de l'administrateur de domaine pour accéder aux partages de réseau sur la machine virtuelle distante. Si l'environnement contient des sauvegardes de machines virtuelles Windows, mais sans données d'identification ou que celles-ci sont

erronées, l'opération échoue. Par conséquent, ne cochez cette case que s'il n'existe aucune sauvegarde de machine virtuelle Windows.

4) Cliquez sur l'URL de l'interface de restauration de fichier pour vérifier si l'interface est accessible.

   A faire : Conservez un enregistrement de l'URL de l'interface de restauration de fichier. Le propriétaire de la machine virtuelle invitée accède à l'interface de restauration de fichier via cette URL.

5) Cliquez sur **OK** pour sauvegarder vos modifications.

- Si vous mettez à jour un environnement existant, procédez comme suit :
  a. Sélectionnez **Editer la configuration de TSM**.
  b. Sur la page Restauration de fichier, suivez les indications ci-après :
     1) Sélectionnez l'option **Activer la restauration de fichier**.
     2) Entrez les informations de contact administrateur affichées dans l'interface de restauration de fichier. Si vous ne voulez pas fournir d'informations de contact, désélectionnez la case à cocher.
     3) Si l'environnement contient des sauvegardes de machines virtuelles Windows, entrez les données d'identification de l'administrateur du domaine Windows. Sinon, ne cochez pas la case et n'entrez pas de données d'identification.

        Conseil : Une opération de restauration de fichier utilise les données d'identification de l'administrateur de domaine pour accéder aux partages de réseau sur la machine virtuelle distante. Si l'environnement contient des sauvegardes de machines virtuelles Windows, mais sans données d'identification ou que celles-ci sont erronées, l'opération échoue. Par conséquent, ne cochez cette case que s'il n'existe aucune sauvegarde de machine virtuelle Windows.

     4) Cliquez sur l'URL de l'interface de restauration de fichier pour vérifier si l'interface est accessible.

        A faire : Conservez un enregistrement de l'URL de l'interface de restauration de fichier. Le propriétaire de la machine virtuelle invitée accède à l'interface de restauration de fichier via cette URL.

     5) Cliquez sur **OK** pour sauvegarder vos modifications.

Résultats

L'environnement est activé pour les opérations de restauration de fichier. Les propriétaires de fichier peuvent restaurer leurs fichiers à l'aide de l'URL permettant d'accéder à l'interface de restauration de fichier de IBM Spectrum Protect.

Configuration des opérations de restauration de fichier sous Linux

Linux

Pour activer la fonction de restauration de fichier lorsque Data Protection for VMware est installé sur un système Linux, un environnement Data Protection for VMware supplémentaire doit être configuré sur un système Windows.

Pourquoi et quand exécuter cette tâche

Lorsque vous exécutez Data Protection for VMware dans un environnement Linux, la fonction de restauration de fichier doit être installée sur un système Windows pour pouvoir être activée.

Procédure

1. Configurez un serveur Windows séparé pour pouvoir utiliser la fonction de restauration de fichier.
2. Installez Data Protection for VMware sur le système Windows. Acceptez les valeurs d'installation par défaut.
3. Lorsque vous configurez Data Protection for VMware sur le système Windows, utilisez les noms de noeuds suivants :
   a. Créez un noeud vCenter nommé `VCENTER_FR`.
   b. Créez un noeud VMCLI nommé `VMCLI_FR`.
   c. Réutilisez le nom de noeud du centre de données provenant de l'environnement Linux.
      Par exemple : `DATACENTER`.
   d. Ne créez pas de noeud de dispositif de transfert de données. Un tel dispositif n'est pas nécessaire pour la fonction de restauration de fichier de ce scénario.
   e. Créez la nouvelle paire de noeuds proxy de montage nommés `REMOTE_FR_MP_WIN` et `REMOTE_FR_MP_LNX`.
4. Sur la page File Restore de l'assistant de configuration, cochez la case `Enable File Restore`.
5. Pour accéder à l'interface de restauration de fichier, ouvrez un navigateur Web et entrez l'URL indiquée par votre administrateur. Par exemple :

   ```
   https:\\hostname:9081\FileRestoreUI
   ```

   où `hostname` désigne le nom d'hôte du système Windows sur lequel Data Protection for VMware est installé.

Résultats

L'exemple suivant illustre les relations de noeud proxy qui existent sur le serveur IBM Spectrum Protect :

```
tsm: SERVER>q proxy

Target Node         Agent Node
---------------     ---------------------------------------------
VCENTER             VMCLI DATACENTER
VCENTER_FR          VMCLI_FR DATACENTER
DATACENTER          VMCLI VMCLI_FR
                     DATAMOVER1
                     REMOTE_MP_WIN REMOTE_MP_LNX
                     REMOTE_FR_MP_WIN REMOTE_FR_MP_LNX
```

Les noeuds supplémentaires qui sont créés pour activer la fonction de restauration de fichiers portent le suffixe `_FR`.

Modification des options des opérations de restauration de fichier

Windows

Pour permettre aux administrateurs de configurer et de contrôler le processus des opérations de restauration de fichier, modifiez les options du fichier `frConfig.props`.

Pourquoi et quand exécuter cette tâche

Procédez comme suit sur le système où l'Interface graphique de Data Protection for VMware vSphere est installée.

Procédure

1. Accédez au répertoire sur lequel réside le fichier `frConfig.props`. Par exemple, ouvrez une invite de commande et lancez la commande suivante :

   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI
   ```

2. Ouvrez le fichier `frConfig.props` à l'aide d'un éditeur de texte en mode administrateur et modifiez les options comme nécessaire. Utilisez les informations de la rubrique «Options de restauration de fichier» pour déterminer les options à modifier.
3. Sauvegardez vos modifications et fermez le fichier `frConfig.props`.

Résultats

Les options modifiées sont appliquées à l'interface de restauration de IBM Spectrum Protect.

Options de restauration de fichier

Les options spécifiées dans le fichier `frConfig.props` contrôlent la configuration, la prise en charge et le processus de restauration des opérations de restauration de fichier.

enable_contact_info=false | true
Indiquez si vous souhaitez fournir des informations de contact de l'administrateur que les propriétaires de fichiers peuvent utiliser pour obtenir une assistance.

false
Les propriétaires de fichiers ne reçoivent pas les informations de contact de l'administrateur. Il s'agit de la valeur par défaut.

true
Les propriétaires de fichiers reçoivent les informations de contact de l'administrateur.

Si vous indiquez **enable_contact_info=true**, vous devez renseigner l'option **contact_info**.

enable_filerestore=false | true
Indiquez si les propriétaires de fichiers peuvent restaurer leurs fichiers depuis une machine virtuelle à l'aide de l'interface de restauration de fichier de IBM Spectrum Protect.

false
Les propriétaires de fichier ne peuvent pas restaurer leurs fichiers depuis l'interface de restauration de fichier de IBM Spectrum Protect. Il s'agit de la valeur par défaut.

true
Les propriétaires de fichier peuvent restaurer leurs fichiers depuis l'interface de restauration de fichier de IBM Spectrum Protect.

maximum_mount_points=*nombre_points_montage*
Indiquez le nombre maximal de points de récupération disponibles pour le compte utilisateur. La valeur minimale est 1 point de récupération. La valeur maximale est de 256 points de montage. La valeur par défaut est de 2 points de montage.

Conseil : Pour empêcher une machine virtuelle d'être montée plusieurs fois pour des opérations de restauration simultanées, affectez à cette option une valeur faible.

mount_session_timeout_minutes=*nombre_minutes*
Spécifiez la durée, en minutes, pendant laquelle une restauration et le point de récupération monté peuvent être inactifs avant que le session ne soit annulée. Une annulation démonte le point de récupération. La valeur maximale est de 8 heures (480 minutes). La valeur par défaut est de 30 minutes.

Conseil : Pour éviter que la session ne soit annulée de manière inattendue, augmentez le nombre de minutes.

restore_info_duration_hours=*nombre_heures*
Indiquez la durée, en heures, pendant laquelle conserver les informations sur l'activité de restauration récente dans l'interface de restauration de fichier de IBM Spectrum Protect. Utilisez la fenêtre d'activité de restauration pour consulter les informations sur les erreurs et sur les tâches réalisées récemment. Ces informations permettent de localiser des fichiers restaurés dernièrement. La valeur maximale est de 14 jours (336 heures). La valeur par défaut est d'une semaine (168 heures).

contact_info=*informations_administrateur*
Indiquez les informations de contact de l'administrateur que les propriétaires de fichiers peuvent utiliser pour assistance. Ces informations sont affichées aux emplacements suivants dans l'interface de restauration de IBM Spectrum Protect :

- Fenêtre de connexion
- Panneau A propos de dans le menu d'aide
- Lien des informations de support dans les messages de l'interface

Vous pouvez remplacer la valeur des options suivantes depuis l'assistant ou le bloc-notes de configuration de l'Interface graphique de Data Protection for VMware vSphere :

- **enable_contact_info**
- **enable_filerestore**
- **contact_info**

Configuration de l'activité de journal pour les opérations de restauration de fichier

Pour permettre aux administrateurs de configurer et de contrôler la mise en forme et la consignation au journal des opérations de restauration de fichier, modifiez les options du fichier `FRLog.config`.

Avant de commencer

Le fichier `FRLog.config` est généré lors du premier accès à l'interface de restauration de fichier de IBM Spectrum Protect.

Pourquoi et quand exécuter cette tâche

Procédez comme suit sur le système sur lequel l'Interface graphique de Data Protection for VMware vSphere est installée.

Procédure

1. Accédez au répertoire sur lequel réside le fichier `FRLog.config`. Ouvrez une invite de commande et lancez la commande suivante :
   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\frGUI\
   ```
2. Ouvrez le fichier `FRLog.config` à l'aide d'un éditeur de texte en mode administrateur et modifiez les options comme nécessaire. Utilisez les informations de la rubrique «Options d'activité du journal de restauration de fichiers» pour déterminer les options à modifier.
3. Sauvegardez vos modifications et fermez le fichier `FRLog.config`.
4. Redémarrez le serveur Web de l'interface graphique :
   a. Cliquez sur **Démarrer** > **Panneau de configuration** > **Outils d'administration** > **Services**.
   b. Cliquez avec le bouton droit sur **Service du serveur Web de Data Protection for VMware**, puis sur **Redémarrer**.

Résultats

Les paramètres et le format choisis sont appliqués au contenu et au format des informations consignées pour les opérations de restauration de fichier.

Options d'activité du journal de restauration de fichiers

Les options du fichier `FRLog.config` contrôlent le contenu et le format de consignation d'informations sur les opérations de restauration de fichiers.

Les options suivantes consignent des informations sur les tâches de restauration de fichiers dans le journal `fr_gui.log` :

MAX_LOG_FILES=*nombre*
Indiquez le nombre maximal de fichiers `fr_gui.log` à conserver. La valeur par défaut est de 8.

MAX_LOG_FILE_SIZE=*nombre*
Indiquez la taille maximale du`fr_gui.log`, en ko. La valeur par défaut est de 8192 ko.

Les options suivantes consignent des informations sur les services de restauration de fichiers dans le journal `fr_api.log`. Ces services sont des services d'API internes associés à l'activité de restauration de fichiers :

API_MAX_LOG_FILES=*nombre*
Indiquez le nombre maximal de fichiers `fr_api.log` à conserver. La valeur par défaut est de 8.

API_MAX_LOG_FILE_SIZE=*nombre*
Indiquez la taille maximale du fichier `fr_api.log`, en ko. La valeur par défaut est de 8192 ko.

API_LOG_FILE_NAME=*nom_fichier_journal_API*
Indiquez le nom du fichier journal de l'API. La valeur par défaut est `fr_api.log`.

API_LOG_FILE_LOCATION=*nom_fichier_journal_API*
Indiquez l'emplacement du fichier journal de l'API. Cet emplacement doit être spécifié en utilisant une barre oblique (/). L'emplacement par défaut est `C:/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs`.

FR.API.LOG=ON | OFF
Indiquez si la consignation au journal doit être activée pour les services de restauration de fichiers.

- Pour activer cette consignation, spécifiez ON. La valeur par défaut est ON.
- Pour désactiver cette consignation, spécifiez OFF.

Pour traiter les incidents susceptibles de survenir lors des opérations de restauration des fichiers, voir Options de trace pour la restauration des fichiers. Les options de trace sont également spécifiées dans le fichier `FRLog.config`.

Configuration d'un noeud de dispositif de transfert de données pour la prise en charge du balisage

Lorsque la prise en charge du balisage est activée sur un noeud de dispositif de transfert de données, les administrateurs peuvent appliquer des balises de protection des données aux objets d'inventaire dans le vCenter VMware.

Avant de commencer

Vérifiez que les conditions requises ci-dessous sont remplies :

- Le serveur VMware vCenter doit être de version 6.0 Update 1 ou de version ultérieure.
- Pour garantir le bon fonctionnement de l'interface graphique Data Protection for VMware vSphere avec le support du balisage, vérifiez que les conditions suivantes sont remplies lors de l'installation de l'interface :
  - Au moins un dispositif de transfert de données et l'interface graphique Data Protection for VMware vSphere doivent être installés sur le même serveur. Ce noeud de dispositif de transfert de données doit être configuré de sorte que les données d'identification du serveur vCenter soient sauvegardées. Vous pouvez exécuter l'assistant de configuration pour sauvegarder le mot de passe du noeud de dispositif de transfert de données ou utiliser la commande **dsmc set password** sur la ligne de commande du dispositif de transfert de données.

    Si vous prévoyez d'utiliser d'autres dispositifs de transfert de données sur des machines virtuelles ou physiques, vous pouvez les installer sur d'autres serveurs. Pour le support du balisage, tous ces dispositifs de transfert de

données doivent également être configurés avec l'option `VMTAGDATAMOVER yes`. Pour fonctionner correctement en tant que dispositifs de transfert de données sensibles aux balises, ils n'ont pas besoin que l'interface graphique Data Protection for VMware vSphere soit installée sur le même serveur.

– Linux Dans le cas des dispositifs de transfert de données fonctionnant sous Linux, veillez à spécifier le répertoire d'installation du dispositif de transfert de données et l'emplacement de la bibliothèque partagée Java `libjvm.so` dans la variable d'environnement `LD_LIBRARY_PATH`. Le chemin d'accès à `libjvm.so` est utilisé pour le support du balisage lorsque vous activez l'option `vmtagdatamover` sur le dispositif de transfert de données. Pour les instructions, consultez Configuration des noeuds de dispositif de transfert de données dans un environnement vSphere.

– Linux Sur les systèmes d'exploitation Linux, l'interface graphique Data Protection for VMware vSphere doit être installée à l'aide du nom d'utilisateur par défaut (`tdpvmware`).

– Sur les clients UNIX et Linux, les mots de passe existants qui figurent dans les fichiers `TSM.PWD` sont migrés vers le nouveau fichier de stockage des mots de passe au même emplacement. Pour les superutilisateurs, l'emplacement par défaut du fichier de stockage des mots de passe est `/etc/adsm`. Pour les utilisateurs non superutilisateur, l'emplacement du fichier de stockage des mots de passe est spécifié par l'option `passworddir`.

  Le fichier `TSM.PWD` est supprimé après la migration.

Remarque : Pour plus d'informations sur l'utilisation des privilèges requis pour la mise en oeuvre des balises, voir Installation des composants Data Protection for VMware

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser les balises de protection des données pour configurer la règle de sauvegarde des machines virtuelles dans les objets d'inventaire VMware. Ces balises de protection des données se présentent sous la forme de paramètres modifiables dans le plug-in client IBM Spectrum Protect vSphere.

Procédure

Utilisez l'une des méthodes suivantes :

Option	Description
Pour configurer un noeud de dispositif de transfert de données à l'aide de l'interface graphique du plug-in vSphere	1. Dans le plug-in vSphere, sélectionnez IBM Spectrum Protect. 2. Sur l'onglet **Configurer**, sélectionnez **Dispositifs de transfert de données**. 3. Dans le panneau **Ajouter un dispositif de transfert de données**, sélectionnez un centre de données dans le menu déroulant. 4. Acceptez les valeurs par défaut ou éditez les paramètres pour **Nom du dispositif de transfert de données**, **Nom d'hôte du dispositif de transfert de données**, **Utilisateur vCenter** et **Mot de passe vCenter**. 5. Une fois les paramètres définis, cliquez sur **Ajouter**. Pour plus de détails, reportez-vous à la rubrique relative à la configuration de noeuds de dispositif de transfert de données avec l'interface graphique du plug-in vSphere dans le document interface graphique Data Protection for VMware vSphere Installation Guide.

Option	Description
Pour configurer un *nouveau* dispositif de transfert de données pour le support du balisage sous Windows ou Linux via l'interface graphique Data Protection for VMware vSphere, procédez comme suit :	1. Sur le système sur lequel est installée l'interface graphique Data Protection for VMware vSphere, démarrez cette dernière en ouvrant un navigateur Web et en entrant l'adresse de serveur Web de l'interface graphique. Par exemple : `https://<adresse_serveur_web_IG>:9081/TsmVMwareUI/` 2. Connectez-vous avec l'ID utilisateur et le mot de passe vCenter. 3. Accédez à l'onglet **Configuration** et sélectionnez l'action **Editer la configuration IBM Spectrum Protect**. 4. Accédez à la page Noeuds du dispositif de transfert de données du bloc-notes de configuration. 5. Ajoutez un noeud de dispositif de transfert de données en effectuant les étapes suivantes : a. Pour le noeud de dispositif de transfert de données pour lequel vous souhaitez configurer le support du balisage, sélectionnez **Créer des services**. Par défaut, l'option **Noeud basé sur une balise** est sélectionnée dans le but d'activer le noeud de dispositif de transfert de données pour le support du balisage. b. Pour désigner le noeud sensible aux balises comme noeud de dispositif de transfert de données par défaut, sélectionnez **Dispositif de transfert de données par défaut**. Le dispositif de transfert de données par défaut sauvegarde chaque nouvelle VM ajoutée à un conteneur du centre de données, à condition que ce conteneur soit déjà dans un ensemble de protection. Il sauvegarde aussi toute VM de l'ensemble de protection à laquelle la balise `Data Mover` n'est pas affectée. **Conseil :** Pour les systèmes Linux, si vous sélectionnez un nouveau noeud de dispositif de transfert de données comme noeud de balisage par défaut, retirez la ligne `vmtagdefaultdatamover` des autres fichiers d'options de dispositif de transfert de données qui sont associés à ce centre de données. c. Cliquez sur **OK** pour sauvegarder vos modifications. Les options `vmtagdatamover` et `vmtagdefaultdatamover` (si elles sont définies) sont ajoutées au fichier d'options du dispositif de transfert de données (`dsm.opt`).
Configurer un noeud de dispositif de transfert de données Windows *existant* pour le support du balisage lorsque le noeud se trouve sur le même serveur que l'interface graphique Data Protection for VMware vSphere	1. Effectuez les étapes 1 à 3 décrites dans les instructions précédentes afin de configurer un nouveau noeud de dispositif de transfert de données pour le support du balisage. 2. Sur la page Noeuds de dispositif de transfert de données, sélectionnez **Noeud à base de balise** pour le noeud pour lequel vous souhaitez activer le support du balisage. 3. **Facultatif :** Pour désigner le noeud sensible aux balises comme noeud de dispositif de transfert de données par défaut, sélectionnez **Dispositif de transfert de données par défaut**.

Option	Description
Configurer un noeud de dispositif de transfert de données Linux *existant* pour le support du balisage ou un noeud de dispositif de transfert de données Linux existant qui se trouve sur un autre serveur que l'interface graphique Data Protection for VMware vSphere	1. Ajoutez l'option `vmtagdatamover yes` dans le fichier d'options du dispositif de transfert de données (`dsm.sys` pour Linux et `dsm.opt` pour Windows). 2. **Facultatif :** Pour désigner le noeud sensible aux balises comme noeud de dispositif de transfert de données par défaut, ajoutez l'option `vmtagdefaultdatamover yes` ou `vmtagdefaultdatamover` *nom_dt* au fichier d'options du dispositif de transfert de données. **Conseil :** Pour les systèmes Linux, si vous sélectionnez un nouveau noeud de dispositif de transfert de données comme noeud de balisage par défaut, retirez la ligne `vmtagdefaultdatamover` des autres fichiers d'options de dispositif de transfert de données qui sont associés à ce centre de données.

Résultats

Une fois le support du balisage activé pour le noeud de dispositif de transfert de données, ce dernier interroge l'inventaire WMware en quête d'informations de balisage lors de l'exécution d'une sauvegarde. Le dispositif de transfert de données sauvegarde ensuite les machines virtuelles en fonction des balises de protection des données définies. Si le noeud de dispositif de transfert de données n'est pas configuré pour le support du balisage, toutes les balises de protection des données sont ignorées au cours d'une opération de sauvegarde.

Information associée:

- `Vmtagdatamover`
- `Vmtagdefaultdatamover`
- Configuration des règles de sauvegarde

Configuration de votre environnement pour les opérations de restauration instantanée de machines virtuelles intégrales

Configurez un réseau iSCSI dédié pour les opérations d'accès instantané et les opérations de restauration instantanée de machines virtuelles intégrales.

Avant de commencer

Utilisez la documentation VMware appropriée (ESXi ou vSphere) pour savoir quelles sont les étapes à suivre pour configurer le commutateur virtuel iSCSI et le réseau de machine virtuelle. Bien que des instructions générales soient fournies, la documentation du produit ne fournit pas d'instructions détaillées sur la manière d'ajouter des réseaux virtuels et des commutateurs virtuels, ni de documentation spécifique à ce sujet. Au moment de la publication, la documentation VMware vSphere ESXi et vCenter 5.5 est disponible sous Documentation VMware ESXi et vCenter Server 5. Les rubriques sur la “Mise en réseau” expliquent comment ajouter et configurer des commutateurs virtuels et des réseaux virtuels.

Important : Ces paramètres de configuration sont fournis pour vous aider à configurer l'environnement VMware afin de réaliser de manière efficace vos opérations de restauration instantanée et d'accès instantané sur les machines virtuelles intégrales. Toutefois, comme ces paramètres s'appliquent aux tâches de configuration VMware et aux interfaces utilisateur VMware, veuillez vous reporter à la documentation VMware appropriée pour obtenir des instructions détaillées.

Pourquoi et quand exécuter cette tâche

Cette procédure requiert un adaptateur iSCSI sur chaque hôte ESXi utilisé pour les opérations de restauration instantanée. Utilisez la documentation VMware appropriée pour configurer l'adaptateur. Au moment de la publication, les procédures suivantes sont disponibles sous la ressource VMware vSphere.

- Pour configurer un adaptateur iSCSI logiciel, suivez les instructions de la procédure VMware “Configuration des adaptateurs iSCSI logiciels”.
- Pour configurer un adaptateur iSCSI matériel, suivez les instructions de la procédure VMware “Configuration des adaptateurs iSCSI matériels indépendants”.

1. Configuration du logiciel iSCSI sur l'hôte ESXi

Procédure

Cette tâche permet de configurer le logiciel iSCSI pour une configuration de base.

1. Connectez-vous à l'hôte ESXi à utiliser pour les opérations de restauration instantanée.
2. Suivez les instructions de cet article de la "Base de connaissances VMware" jusqu'à ce que l'adaptateur iSCSI soit activé : http://kb.vmware.com/kb/1008083
   IBM Spectrum Protect détecte automatiquement le serveur cible iSCSI.
3. Vérifiez que l'adresse IP de l'adaptateur iSCSI (sur l'hôte ESXi) correspond à l'adresse de sous-réseau utilisée par le dispositif de transfert de données.
4. Vérifiez que la licence de Storage vMotion est activée sur l'hôte ESXi.

Que faire ensuite

Une fois que le logiciel iSCSI est configuré sur l'hôte ESXi, installez et configurez des applications sur le système du dispositif de transfert de données.

2. Installation et configuration des applications sur le dispositif de transfert de données

Avant de commencer

Si l'agent de récupération et le dispositif de transfert de données IBM Spectrum Protect sont déjà installés et configurés sur le système du dispositif de transfert de données, commencez à l'étape 3.

Procédure

Cette tâche configure le système du dispositif de transfert de données avec les applications et les paramètres requis pour les opérations de restauration instantanée.

1. Installez l'agent de récupération et le dispositif de transfert de données IBM Spectrum Protect sur le système du dispositif de transfert de données.
   A l'étape 4 de la procédure Installation de Data Protection for VMware, sélectionnez le type d'installation **Installer un dispositif de transfert de données complet pour la protection d'application invitée**.
2. Configurez le dispositif de transfert de données.
   Suivez les instructions de configuration du dispositif de transfert de données dans la documentation du client.

3. Définissez l'adresse IP du serveur iSCSI :
   a. Accédez au fichier `C:\Program Files\Tivoli\TSM\baclient\dsm.opt` et spécifiez le paramètre suivant :

      ```
      VMISCSIServeraddress=<Adresse IP de la carte réseau sur le système
      du dispositif de transfert de données
      exposant les cibles iSCSI.>
      ```

      Si le système de votre dispositif de transfert de données possède plus d'une carte réseau, assurez-vous de spécifier la carte réseau correcte pour le réseau iSCSI.

Que faire ensuite

Une fois que le système du dispositif de transfert est configuré, établissez une connexion entre l'interface de ligne de commande de Recovery Agent et l'interface graphique de Recovery Agent.

3. Définition des connexions de Recovery Agent

Avant de commencer

L'interface de ligne de commande de Recovery Agent V7.1.x peut être affichée comme une interface de programme d'application de ligne de commande sur l'interface graphique de Recovery Agent. Vous pouvez utiliser l'interface de ligne de commande de Recovery Agent pour communiquer avec l'interface graphique de Recovery Agent.

Procédure

Cette tâche établit une connexion entre l'interface de ligne de commande de Recovery Agent et l'interface graphique de Recovery Agent.

1. Démarrez l'interface de ligne de commande de Recovery Agent sur le système du dispositif de transfert de données.
   Dans le menu **Démarrer** de Windows, cliquez sur **Programmes** > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect Recovery Agent**.
2. Dans la fenêtre d'invite de commande, entrez la commande suivante :

   ```
   RecoveryAgentShell.exe -c set_connection mount_computer <Adresse IP
   de la carte réseau sur le système du dispositif de transfert de données
   exposant les cibles iSCSI.>
   ```

   Cette commande établit une connexion entre l'interface de ligne de commande de Recovery Agent et l'interface graphique de Recovery Agent.

Que faire ensuite

Une fois la connexion établie, configurez un réseau iSCSI dédié.

4. Configuration d'un réseau iSCSI dédié pour l'hôte ESXi et le dispositif de transfert de données

Avant de commencer

Tenez compte des instructions suivantes avant de poursuivre cette tâche :

- Utilisez un réseau iSCSI dédié pour les opérations de restauration instantanée.
- Chaque hôte ESXi utilisé pour les opérations de restauration instantanée doit avoir une seconde carte réseau physique disponible. Cette seconde carte réseau est liée à l'adaptateur iSCSI logiciel de l'hôte ESXi respectif.
- Le système du dispositif de transfert de données qui s'exécute sur une machine virtuelle doit avoir une seconde carte réseau disponible. Cette seconde carte réseau est liée à l'adaptateur iSCSI logiciel de l'hôte ESXi.
- Chaque hôte ESXi utilisé pour des opérations de restauration instantanée doit avoir un magasin de données VMware secondaire disponible. Ce magasin de données temporaire contient les informations de configuration et les données de la machine virtuelle qui est créée lors de l'opération.

Procédure

Cette tâche configure un réseau iSCSI dédié pour l'hôte ESXi et pour le dispositif de transfert de données qui s'exécute sur une machine virtuelle.

1. Connectez-vous à l'hôte ESXi à utiliser pour les opérations de restauration instantanée.
2. Configurez le commutateur virtuel du réseau iSCSI.
   Ces étapes utilisent *vSwitch1* comme commutateur virtuel.
   a. Sélectionnez **VMkernel Network Adapter** sous **`Connection Type`**.
      Le réseau iSCSI nécessite ce type de connexion.
   b. Sélectionnez **Create a vSphere standard switch** sous **`VMkernel Network Access`**.
   c. Sélectionnez **Network Label** sous **`VMkernel Connection Settings`**.
      Spécifiez une étiquette indiquant que *vSwitch1* et ce réseau sont réservés à votre trafic iSCSI.
      Par exemple : *VMkernel iSCSI*.
   d. Spécifiez une adresse IP et un masque de sous-réseau pour *vSwitch1* dans **`VMkernel IP Connection Settings`**.
      Ne modifiez pas les valeurs de **`Subnet Mask`** ni de **`VMkernel Default Gateway`**.
   e. Spécifiez le port du noyau permettant au réseau iSCSI de fonctionner.
3. Configurez le commutateur virtuel du réseau de machine virtuelle.
   Ces étapes utilisent *vSwitch0* comme commutateur virtuel.
   a. Sélectionnez **Virtual Machine** sous **`Connection Type`**.
   b. Sélectionnez **Create a vSphere standard switch** sous **`VMkernel Network Access`**.
   c. Accédez à l'onglet **Port Group Properties** et sélectionnez **Network Label**.
      Spécifiez la même étiquette que celle qui a été spécifiée pour le réseau de machine virtuelle de *vSwitch1*.
      Par exemple : *VMkernel iSCSI*.
4. Associez l'adaptateur iSCSI que vous venez de créer à **`VMkernel Network Adapter`**.
   Suivez les instructions de la procédure VMware “Lier des adaptateurs iSCSI et

des adaptateurs VMkernel". Au moment de la publication, cette procédure était disponible sous Documentation VMware ESXi et vCenter Server 5.

Conseil : Si le délai d'attente expire durant l'analyse des périphériques iSCSI, réduisez le nombre de périphériques iSCSI connectés à l'hôte ESXi. Relancez ensuite l'analyse des périphériques iSCSI.

5. Vérifiez que les propriétés de liaison de l'adaptateur iSCSI sont correctes.
   a. Accédez à **Hardware** > **Storage Adapters** dans le client VMware vSphere.
   b. Cliquez avec le bouton droit de la souris sur l'adaptateur iSCSI et sélectionnez **iSCSI Initiator Properties**. Vérifiez que les propriétés de liaison suivantes existent :

Tableau 10. Paramètres du réseau iSCSI

Réseau de machine virtuelle	Réseau iSCSI
Standard Switch: *vSwitch0*	**Standard Switch**: *vSwitch1*
Virtual Machine Port Group: *VM Network*	**VMkernel Port**: *VMkernel iSCSI* **Conseil :** *VMkernel iSCSI* est lié à **VMkernel Adapter**: *vmk1*, qui est sur **Physical Network Adapter**: *vmnic1*.
Physical Adapter: *vmnic0*	**VMkernel Network Adapter**: *vmk1*
	Physical Network Adapter: *vmnic1*
	Virtual Network Adapter **IP address**: 192.168.42.x (sous-réseau du réseau iSCSI)

Résultats

Un réseau iSCSI dédié est prêt pour les opérations d'accès instantané et les opérations de restauration instantanée de machines virtuelles intégrales.

Configuration des paramètres de sécurité pour Data Protection for VMware

Les dispositifs de transfert de données Data Protection for VMware, l'interface de ligne de commande vmcli et les composants interface graphique Data Protection for VMware vSphere requièrent une configuration pour permettre une connexion sécurisée avec le serveur IBM Spectrum Protect.

Configuration des paramètres de sécurité pour connecter les noeuds VMCLI et de dispositif de transfert de données au serveur IBM Spectrum Protect

Il existe plusieurs options de configuration qui concernent les paramètres de sécurité Data Protection for VMware pour les noeuds VMCLI et de dispositif de transfert de données lors d'une connexion à serveur IBM Spectrum Protect version 7.1.8, 8.1.2 ou versions ultérieures. L'acceptation des valeurs par défaut pour ces options, qui configure de façon transparente ces composants pour une sécurité renforcée, est recommandée pour la plupart des cas d'utilisation.

Configuration en utilisant les paramètres de sécurité par défaut (scénario raccourci)

Le scénario raccourci détaille les options de configuration impactant la sécurité de la connexion au serveur des noeuds VMCLI et de dispositif de transfert de données pour différents cas d'utilisation quand les valeurs par défaut sont acceptées. Ce scénario réduit les étapes du processus de configuration aux points d'extrémité.

Ce scénario obtient automatiquement des certificats du serveur quand le noeud se connecte pour la première fois, en supposant que le paramètre serveur IBM Spectrum Protect **SESSIONSECURITY** est défini sur **TRANSITIONAL**, ce qui est la valeur par défaut à la première connexion. Vous pouvez suivre ce scénario, que vous mettiez d'abord le serveur IBM Spectrum Protect au niveau de la version 7.1.8 (et niveaux ultérieurs) et de la version 8.1.2 (et niveaux ultérieurs) pour ensuite procéder à la même opération pour Data Protection for VMware, ou inversement.

Avertissement : vous ne pouvez pas suivre ce scénario si le serveur IBM Spectrum Protect est configuré pour l'authentification LDAP. Si LDAP est utilisé, vous pouvez importer manuellement les certificats nécessaires à l'aide de l'utilitaire dsmcert. Pour plus d'informations, voir «Configuration sans distribution automatique des certificats», à la page 62.

Options de noeud de dispositif de transfert de données affectant la sécurité de session

Les options dsmc suivantes spécifient les paramètres de sécurité pour le noeud de dispositif de transfert de données. Pour plus d'informations sur ces options, voir Informations de référence sur les options client.

- `SSLREQUIRED`. La valeur par défaut `Par défaut` active les connexions de sécurité de session existantes antérieures à la version 7.1.8 ou 8.1.2 et configure automatiquement le dispositif de transfert de données Data Protection for VMware pour une connexion sécurisée à un serveur version 7.1.8 ou 8.1.2 ou à un serveur ultérieur en utilisant TLS pour l'authentification.
- `SSLACCEPTCERTFROMSERV`. La valeur par défaut `Oui` permet au dispositif de transfert de données d'accepter automatiquement un certificat public auto-signé en provenance du serveur et de configurer automatiquement le dispositif de transfert de données pour qu'il utilise ce certificat quand le dispositif se connecte à un serveur version 7.1.8, 8.1.2 ou à un serveur ultérieur.
- `SSL`. La valeur par défaut `Non` indique qu'aucun chiffrement n'est utilisé quand les données sont transférées entre le dispositif de transfert de données et un serveur antérieur à la version 7.1.8 ou 8.1.2. Quand le dispositif de transfert de données se connecte à un serveur version 7.1.8, 8.1.2 ou ultérieure, la valeur par défaut `Non` indique que les données objet ne sont pas chiffrées. Toutes les autres informations sont chiffrées, au moment où le dispositif de transfert de données communique avec le serveur. La valeur `Oui` indique que TLS est utilisé pour chiffrer toutes les informations, dont les données objet, quand le dispositif de transfert de données communique avec le serveur.
- `SSLFIPSMODE`. La valeur par défaut `Non` indique qu'aucune bibliothèque TLS certifiée FIPS (Federal Information Processing Standards) n'est requise.

De plus, les options suivantes ne s'appliquent que lorsque le dispositif de transfert de données utilise une connexion TLS vers un serveur antérieur à la version 7.1.8 ou 8.1.2. Elles sont ignorées si cette connexion s'effectue vers un serveur ultérieur.

- `SSLDISABLELEGACYTLS`. Si l'option a la valeur `Non`, le dispositif de transfert de données ne requiert pas TLS 1.2 pour les sessions SSL. Il autorise les connexions

avec TLS 1.1 et les protocoles SSL de niveau inférieur. Lorsque le dispositif de transfert de données communique avec un serveur IBM Spectrum Protect version 7.1.7 ou 8.1.1 ou antérieure, l'option a par défaut la valeur `Non`.

- `LANFREESSL`. La valeur par défaut `Non` indique que le dispositif de transfert de données n'utilise pas TLS lorsqu'il communique avec l'agent de stockage quand le transfert de données hors réseau local est configuré.
- `REPLSSLPORT`. Spécifie l'adresse de port TCP/IP qui est activée pour TLS quand le dispositif de transfert de données communique avec le serveur de réplication cible.

Options de noeud VMCLI affectant la sécurité de session

Les paramètres suivants portent sur la sécurité du noeud VMCLI. Pour plus d'informations sur ces options, voir Paramètres du profil.

- `VE_TSM_SSL`. La valeur par défaut `NON` indique qu'aucun chiffrement n'est utilisé quand les données sont transférées entre le dispositif de transfert de données et un serveur antérieur à la version 7.1.8 ou 8.1.2. Définissez cette valeur sur `OUI` si vous voulez vous servir de TLS pour chiffrer toutes les informations lors d'une connexion à un serveur antérieur à V7.1.8.
- `VE_TSM_SSLACCEPTCERTFROMSERV`. La valeur par défaut `OUI` permet à l'interface d'accepter automatiquement un certificat public auto-signé en provenance du serveur et de configurer automatiquement l'interface pour qu'elle utilise ce certificat quand le dispositif se connecte à un serveur version 7.1.8, 8.1.2 ou un serveur ultérieur.
- `VE_TSM_SSLREQUIRED`. La valeur par défaut `PAR DEFAUT` active les connexions de sécurité de session existantes antérieures à la version 7.1.8 ou 8.1.2 et configure automatiquement l'interface pour une connexion sécurisée à un serveur version 7.1.8, 8.1.2 ou un serveur ultérieur en utilisant TLS pour l'authentification.

Cas d'utilisation pour les paramètres de sécurité par défaut

- Dans un premier temps, le serveur est mis au niveau de la version 7.1.8, 8.1.2 ou d'une version ultérieure. Ensuite, Data Protection for VMware est mis à niveau. Les noeuds VMCLI et de dispositif de transfert de données *n'utilisent pas* de communications SSL :
  - Les options de sécurité pour les noeuds VMCLI et de dispositif de transfert de données n'ont pas besoin d'être modifiées.
  - La configuration est automatiquement mise à jour pour utiliser TLS quand les noeuds s'authentifient au serveur.
- Dans un premier temps, le serveur est mis au niveau de la version 7.1.8, 8.1.2 ou d'une version ultérieure. Ensuite, Data Protection for VMware est mis à niveau. Les noeuds VMCLI et de dispositif de transfert de données *utilisent* des communications SSL :
  - Les options de sécurité pour les noeuds VMCLI et de dispositif de transfert de données n'ont pas besoin d'être modifiées.
  - Les communications SSL avec le certificat public du serveur existant continuent d'être utilisées.
  - Les communications SSL sont automatiquement renforcées pour utiliser le niveau TLS qui est requis par le serveur.
- Dans un premier temps, Data Protection for VMware est mis au niveau de la version 7.1.8, 8.1.2 ou d'une version ultérieure. Le serveur est mis à niveau ultérieurement. Les noeuds VMCLI et de dispositif de transfert de données *n'utilisent pas* de communications SSL :

  - Les options de sécurité pour les noeuds VMCLI et de dispositif de transfert de données n'ont pas besoin d'être modifiées.
  - Le protocole d'authentification existant continue d'être utilisé sur les serveurs dont les niveaux sont antérieurs à la version 7.1.8 ou 8.1.2.
  - La configuration est automatiquement mise à jour pour utiliser TLS quand les noeuds s'authentifient au serveur après la mise à niveau du serveur vers la version 7.1.8, 8.1.2 ou ultérieure.
- Dans un premier temps, Data Protection for VMware est mis au niveau de la version 7.1.8, 8.1.2 ou d'une version ultérieure. Le serveur est mis à niveau ultérieurement. Les noeuds VMCLI et de dispositif de transfert de données *utilisent* des communications SSL :
  - Les options de sécurité pour les noeuds VMCLI et de dispositif de transfert de données n'ont pas besoin d'être modifiées.
  - Les communications SSL avec le certificat public du serveur existant continuent d'être utilisées avec les serveurs aux niveaux antérieurs à la version 7.1.8 ou 8.1.2.
  - Les communications SSL sont automatiquement renforcées pour utiliser le niveau TLS qui est requis par le serveur après la mise à niveau de ce dernier vers la version 7.1.8, 8.1.2 ou ultérieure.
- Dans un premier temps, Data Protection for VMware est mis au niveau de la version 7.1.8, 8.1.2 ou d'une version ultérieure. Ensuite, les noeuds VMCLI et de dispositif de transfert de données se connectent à plusieurs serveurs. Les serveurs sont mis à niveau à différents moments.
  - Les options de sécurité pour les noeuds VMCLI et de dispositif de transfert de données n'ont pas besoin d'être modifiées.
  - Les noeuds VMCLI et de dispositif de transfert de données utilisent un protocole d'authentification et de sécurité de session existant sur les serveurs de versions antérieures à la version 7.1.8 ou 8.1.2 et une mise à niveau automatique s'exécute pour utiliser l'authentification TLS lors de la connexion initiale à un serveur version 7.1.8, 8.1.2 ou ultérieure. La sécurité de session est gérée par serveur.
- Nouvelle installation client, serveur version 7.1.8, 8.1.2 ou ultérieure :
  - Configurez Data Protection for VMware en fonction d'une nouvelle installation.
  - Les valeurs par défaut pour les options de sécurité configurent automatiquement les noeuds VMCLI et de dispositif de transfert de données pour une authentification de session chiffrée TLS.
  - Définissez le paramètre SSL à `Oui` si un chiffrement est requis pour tous les transferts de données entre le client et le serveur.
- Nouvelle installation client, la version du serveur est antérieure à 7.1.8 ou 8.1.2 :
  - Configurez le client en fonction d'une nouvelle installation client.
  - Acceptez les valeurs par défaut pour les paramètres de sécurité de session client si le chiffrement SSL de tous les transferts de données n'est pas requis.
    - Un protocole d'authentification non SSL est utilisé jusqu'à ce que le serveur soit mis au niveau de la version 7.1.8, 8.1.2 ou ultérieure.
  - Définissez le paramètre SSL à `Oui` si un chiffrement est requis pour tous les transferts de données entre le dispositif de transfert de données et le serveur puis effectuez une configuration manuelle pour SSL.
    - Voir la rubrique traitant de la configuration des communications client/serveur Tivoli Storage Manager avec Secure Sockets Layer pour des instructions de configuration.

- Les communications SSL sont automatiquement renforcées pour utiliser le niveau TLS qui est requis par le serveur après la mise à niveau de ce dernier vers la version 7.1.8, V8.1.2 ou ultérieure.

Configuration sans distribution automatique des certificats

Ce scénario détaille les options de configuration impactant la sécurité des noeuds VMCLI et de dispositif de transfert de données quand la distribution automatique de certificats depuis le serveur n'est pas acceptable. Par exemple, la distribution automatique des certificats depuis le serveur n'est pas admise si le serveur est configuré pour utiliser l'authentification LDAP ou si les certificats doivent être signés par une autorité de certification.

Options affectant la sécurité de session

Les options des paramètres de sécurité sont les mêmes que celles décrites dans la rubrique «Configuration en utilisant les paramètres de sécurité par défaut (scénario raccourci)», à la page 59, sauf que vous devez définir l'option `SSLACCEPTCERTFROMSERV` à `Non` pour vous assurer que le noeud de dispositif de transfert de données n'accepte pas automatiquement un certificat public auto-signé en provenance du serveur quand ce noeud se connecte à un serveur version 7.1.8, 8.1.2 ou à un serveur ultérieur.

Cas d'utilisation pour la configuration des noeuds du dispositif de transfert de données sans distribution automatique des certificats

Si une distribution automatique des certificats n'est pas possible ou souhaitée, servez-vous de l'utilitaire dsmcert pour importer le certificat. Procurez-vous le certificat nécessaire depuis le serveur IBM Spectrum Protect ou depuis une autorité de certification. L'autorité de certification peut provenir d'une société comme VeriSign ou Thawte ou il peut s'agir d'une autorité de certification interne qui est gérée au sein de votre société.

Si les noeuds VMCLI et de dispositif de transfert de données se trouvent sur la même machine, un seul certificat est requis. Si les noeuds sont sur des machines séparées, un certificat est nécessaire sur chaque machine.

- Dans un premier temps, le serveur est mis au niveau de la version 7.1.8 ou 8.1.2. Ensuite, Data Protection for VMware est mis à niveau. Les noeuds de dispositif de transfert de données existants *n'utilisent pas* de communications SSL :
  - Définissez l'option `SSLACCEPTCERTFROMSERV` sur la valeur `Non`.
  - Procurez-vous le certificat nécessaire depuis le serveur IBM Spectrum Protect ou depuis une autorité de certification. Voir la rubrique traitant de la configuration des communications client/serveur Tivoli Storage Manager avec Secure Sockets Layer pour des instructions de configuration.
- Dans un premier temps, le serveur est mis au niveau de la version 7.1.8 ou 8.1.2. Ensuite, Data Protection for VMware est mis à niveau. Les noeuds de dispositif de transfert de données existants *utilisent* des communications SSL :
  - Les options de sécurité pour les noeuds de dispositif de transfert de données n'ont pas besoin d'être modifiées. Si les noeuds disposent déjà d'un certificat serveur pour les communications SSL, l'option `SSLACCEPTCERTFROMSERV` ne s'applique pas.
  - Les communications SSL avec le certificat public du serveur existant continuent d'être utilisées.
  - Les communications SSL sont automatiquement renforcées pour utiliser le niveau TLS qui est requis par le serveur.

- Dans un premier temps, Data Protection for VMware est mis au niveau de la version 7.1.8 ou 8.1.2. Le serveur est mis à niveau ultérieurement. Les noeuds de dispositif de transfert de données existants *n'utilisent pas* de communications SSL :
  - Définissez l'option `SSLACCEPTCERTFROMSERV` sur la valeur `Non`.
  - Le protocole d'authentification existant continue d'être utilisé sur les serveurs dont les niveaux sont antérieurs à la version 7.1.8 ou 8.1.2.
  - Avant que les noeuds de dispositif de transfert de données ne se connectent à un serveur version 7.1.8, 8.1.2 ou à un serveur ultérieur :
    - Procurez-vous le certificat nécessaire depuis le serveur IBM Spectrum Protect ou depuis une autorité de certification. Voir la rubrique traitant de la configuration des communications client/serveur Tivoli Storage Manager avec Secure Sockets Layer pour des instructions de configuration.
- Dans un premier temps, Data Protection for VMware est mis au niveau de la version 7.1.8 ou 8.1.2. Le serveur est mis à niveau ultérieurement. Les noeuds de dispositif de transfert de données existants *utilisent* des communications SSL :
  - Les options de sécurité pour les noeuds de dispositif de transfert de données n'ont pas besoin d'être modifiées. Si les noeuds disposent déjà d'un certificat serveur pour les communications SSL, l'option `SSLACCEPTCERTFROMSERV` ne s'applique pas.
  - Les communications SSL avec le certificat public du serveur existant continuent d'être utilisées avec les serveurs aux niveaux antérieurs à la version 7.1.8 ou 8.1.2.
  - Les communications SSL sont automatiquement renforcées pour utiliser le niveau TLS qui est requis par le serveur après la mise à niveau de ce dernier vers la version 7.1.8, V8.1.2 ou ultérieure.
- Dans un premier temps, Data Protection for VMware est mis au niveau de la version 7.1.8 ou 8.1.2. Ensuite, les noeuds de dispositif de transfert de données se connectent à plusieurs serveurs. Les serveurs sont mis à niveau à différents moments.
  - Définissez l'option `SSLACCEPTCERTFROMSERV` sur la valeur `Non`.
  - Le protocole d'authentification existant continue d'être utilisé sur les serveurs dont les niveaux sont antérieurs à la version 7.1.8 ou 8.1.2 .
  - Avant que les noeuds de dispositif de transfert de données ne se connectent à un serveur 7.1.8, 8.1.2 ou un serveur ultérieur ou si des communications SSL sont requises à un niveau de serveur quelconque :
    - Procurez-vous le certificat nécessaire depuis le serveur IBM Spectrum Protect ou depuis une autorité de certification. Voir la rubrique traitant de la configuration des communications client/serveur Tivoli Storage Manager avec Secure Sockets Layer pour des instructions de configuration.
  - Les noeuds de dispositif de transfert de données utilisent un protocole d'authentification et de sécurité de session existant sur les serveurs de versions antérieures à la version 7.1.8 ou 8.1.2 et une mise à niveau automatique s'exécute pour utiliser l'authentification TLS lors de la connexion initiale à un serveur version 7.1.8, 8.1.2 ou ultérieure. La sécurité de session est gérée par serveur.
- Nouvelle installation Data Protection for VMware, serveur 7.1.8, 8.1.2 ou version ultérieure :
  - Configurez Data Protection for VMware en fonction d'une nouvelle installation.
  - Définissez l'option `SSLACCEPTCERTFROMSERV` sur la valeur `Non`.

- Procurez-vous le certificat nécessaire depuis le serveur IBM Spectrum Protect ou depuis une autorité de certification. Voir la rubrique traitant de la configuration des communications client/serveur Tivoli Storage Manager avec Secure Sockets Layer pour des instructions de configuration.
- Définissez le paramètre SSL à `Oui` si un chiffrement est requis pour tous les transferts de données entre le dispositif de transfert de données et le serveur.

- Nouvelle installation Data Protection for VMware, la version du serveur est antérieure à la version 7.1.8 ou 8.1.2, des sessions chiffrées SSL *sont* requises :
  - Configurez Data Protection for VMware en fonction d'une nouvelle installation.
  - Définissez le paramètre SSL à `Oui`.
  - Procurez-vous le certificat nécessaire depuis le serveur IBM Spectrum Protect ou depuis une autorité de certification. Voir la rubrique traitant de la configuration des communications client/serveur Tivoli Storage Manager avec Secure Sockets Layer pour des instructions de configuration.
- Nouvelle installation Data Protection for VMware, la version du serveur est antérieure à la version 7.1.8 ou 8.1.2, *aucune* session chiffrée SSL *n'est* requise :
  - Configurez Data Protection for VMware en fonction d'une nouvelle installation.
  - Définissez l'option `SSLACCEPTCERTFROMSERV` sur la valeur `Non`.
    - Un protocole d'authentification non SSL est utilisé jusqu'à ce que le serveur soit mis au niveau de la version 7.1.8, 8.1.2 ou ultérieure.
  - Avant que les noeuds de dispositif de transfert de données ne se connectent à un serveur version 7.1.8, 8.1.2 ou à un serveur ultérieur :
    - Procurez-vous le certificat nécessaire depuis le serveur IBM Spectrum Protect ou depuis une autorité de certification. Voir la rubrique traitant de la configuration des communications client/serveur Tivoli Storage Manager avec Secure Sockets Layer pour des instructions de configuration.

Configuration des communications de l'Interface graphique de Data Protection for VMware vSphere en utilisant TLS (Transport Layer Security)

L'Interface graphique de Data Protection for VMware vSphere se sert du protocole TLS pour fournir des communications sécurisées avec les navigateurs Web, le serveur VMware vCenter et éventuellement, le serveur IBM Spectrum Protect.

Pourquoi et quand exécuter cette tâche

Pour les communications avec les navigateurs Web et le serveur VMware VCenter, le protocole TLS est toujours activé. Lors de l'installation de Data Protection for VMware, un certificat numérique TLS autosigné est généré puis utilisé pour les connexions.

Vous pouvez aussi vous servir d'un certificat qui est signé par une autorité de certification pour communiquer avec les navigateurs Web. Data Protection for VMware Pour utiliser un certificat tiers, voir la rubrique relative à l'utilisation d'un certificat tiers pour des sessions de navigateur Web.

Pour les communications avec le serveur IBM Spectrum Protect, l'utilisation du protocole TLS dépend de la version du serveur.

Si vous utilisez le serveur IBM Spectrum Protect version 7.1.7, 8.1.1 ou une version antérieure

L'utilisation du protocole TLS pour communiquer avec le serveur est facultative. Vous pouvez activer manuellement l'Interface graphique de Data Protection for VMware vSphere pour communiquer avec le serveur via le protocole TLS en créant ou mettant à jour le magasin de clés certifiées, puis en important un certificat comme décrit dans «Activation de la communication sécurisée avec le serveur IBM Spectrum Protect».

Si vous utilisez le serveur IBM Spectrum Protect version 7.1.8, 8.1.2 ou une version ultérieure

Le protocole TLS est requis. Dans la plupart des cas, le magasin de clés certifiées est créé automatiquement à la première utilisation en se servant des paramètres de sécurité par défaut qui sont décrits dans «Configuration en utilisant les paramètres de sécurité par défaut (scénario raccourci)», à la page 59. Toutefois, dans certains scénarios, il peut s'avérer nécessaire de créer manuellement le magasin de clés certifiées.

Important : Le scénario raccourci obtient les certificats quand l'Interface graphique de Data Protection for VMware vSphere communique avec le serveur pour la première fois, en supposant que le paramètre serveur IBM Spectrum Protect **SESSIONSECURITY** est défini sur **TRANSITIONAL**, ce qui est la valeur par défaut à la première connexion. Une fois que l'interface graphique est connectée au serveur, le paramètre **SESSIONSECURITY** est défini sur **STRICT**. Puisque cette interface utilise l'ID administrateur de serveur pour se connecter au serveur, si une autre entité s'est servi de cet ID pour se connecter, un message d'erreur s'affiche dans l'interface lors de la tentative de connexion au serveur. Pour résoudre ce problème, définissez à nouveau le paramètre **SESSIONSECURITY** sur **TRANSITIONAL**.

Activation de la communication sécurisée avec le serveur IBM Spectrum Protect

Si vous utilisez le serveur IBM Spectrum Protect version 7.1.7 ou antérieure ou 8.1.2 ou antérieure, la connexion au serveur via le protocole TLS est facultative et si vous voulez activer les communications de l'Interface graphique de Data Protection for VMware vSphere avec le serveur en utilisant le protocole, vous devez procéder à cette opération manuellement.

Avant de commencer

Obtenez une copie du certificat auprès de l'administrateur du serveur.

Pourquoi et quand exécuter cette tâche

Si vous utilisez le serveur version 7.1.8, 8.1.2 ou ultérieure, le protocole TLS est requis et un fichier de clés certifiées avec un certificat est automatiquement créé à la première utilisation en se servant des paramètres de sécurité par défaut qui sont décrits dans «Configuration en utilisant les paramètres de sécurité par défaut (scénario raccourci)», à la page 59. Toutefois, dans certains scénarios, il est possible qu'il vous soit demandé de créer manuellement le fichier de clés certifiées et de configurer l'Interface graphique de Data Protection for VMware vSphere, comme expliqué dans cette rubrique.

La procédure suivante utilise l'outil de gestion de clés et de certificats Java™ **keytool**.

Sur les systèmes d'exploitation Linux, il se trouve dans le répertoire `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

Sur les systèmes d'exploitation Microsoft Windows, cet outil se trouve dans le répertoire `C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre\bin`.

Vous devrez peut-être spécifier le chemin d'accès complet lors de l'exécution de la commande **keytool**.

Procédure

1. A partir de la ligne de commande, accédez au répertoire où se trouve le fichier de clés certifiées :
   - Sous Linux : `/opt/tivoli/tsm/tdpvmware/common/scripts/`
   - Sous Windows : `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\`
2. Créez le fichier de clés certifiées et importez le certificat à l'aide de la commande suivante :

   ```
   keytool -importcert -alias mon-cert -file cert.pem -keystore
   tsm-ve-truststore.jks -storepass mot de passe
   ```

   Où :

   -alias *mon-cert*
   : Alias unique qui identifie le certificat dans le fichier de clés certifiées.

   -file *cert.pem*
   : Fichier contenant le certificat autosigné du serveur ou le certificat racine de l'autorité de certification.

   -storepass *mot de passe*
   : Mot de passe du fichier de clés. Assurez-vous de mémoriser ce mot de passe pour une utilisation ultérieure.
3. Démarrez l'interface graphique de Data Protection for VMware vSphere et accédez à la fenêtre Configuration.
   - Si vous créez une configuration initiale, cliquez sur **Tâches** > **Exécuter l'assistant de configuration IBM Spectrum Protect** et accédez à la page Données d'identification du serveur.
   - Si vous modifiez une configuration existante, cliquez sur **Tâches** > **Modifier la configuration IBM Spectrum Protect** et accédez à la page Données d'identification du serveur.
4. Entrez le numéro de port dans la zone **Port Admin IBM Spectrum Protect**. Il s'agit du port du serveur qui permet les connexions administratives à l'aide des protocoles SSL ou TLS.
5. Sélectionnez **Utiliser des communications chiffrées sur le port d'administration**.
6. Si vous souhaitez utiliser ce paramètre pour des sessions ultérieures de l'interface graphique, sélectionnez **Enregistrer l'ID admin, le mot de passe et les paramètres de port**.
7. Cliquez sur **OK** pour appliquer les modifications.

Utilisation d'un certificat provenant d'une autorité de certification

Pour utiliser un certificat qui est signé par une autorité de certification, vous devez effectuer plusieurs étapes.

Pourquoi et quand exécuter cette tâche

Les procédures suivantes utilisent l'outil standard de gestion de clés et de certificats **keytool**.

Sur les systèmes d'exploitation Linux, il se trouve dans le répertoire `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

Sur les systèmes d'exploitation Microsoft Windows, il se trouve dans le répertoire `C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre`.

Vous devrez peut-être spécifier le chemin d'accès complet lors de l'exécution de **keytool** à partir de la ligne de commande.

Procédure

1. Accédez au fichier de clés.
2. Créez une demande de signature de certificat.
3. Envoyez la demande de signature de certificat à l'autorité de certification pour signature.
4. Recevez le certificat signé dans l'interface graphique de Data Protection for VMware vSphere.

Accès au fichier de clés :

Les certificats sont stockés dans un fichier de clés Java. Le contenu du fichier de clés est protégé par un mot de passe. Pour manipuler les certificats dans le fichier de clés, vous devez accéder au fichier de clés.

Pourquoi et quand exécuter cette tâche

Le certificat autosigné et le mot de passe du fichier de clés par défaut sont générés automatiquement lors de l'installation. Il est donc peu probable que vous connaissiez le mot de passe initial.

Procédez comme suit pour remplacer le fichier de clés d'origine par un nouveau fichier de clés et un nouveau certificat autosigné. Le nouveau fichier de clés est protégé par un mot de passe de votre choix.

Si vous connaissez déjà le mot de passe du fichier de clés, ignorez cette procédure.

Procédure

1. Arrêtez le service interface graphique de Data Protection for VMware vSphere.
2. A partir de la ligne de commande, accédez au répertoire où se trouve le fichier de clés.
   - Sous Linux : `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - Sous Windows : `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
3. Faites une copie de sauvegarde du fichier de clés (`key.jks`) en le renommant ou le déplaçant vers un autre emplacement.

4. Exécutez la commande suivante pour créer un fichier de clés et un certificat autosigné :

   ```
   keytool -genkeypair -alias vekey -dname
   CN=nom de domaine complet,OU=Tivoli_Storage_Manager_for_VMware,O=IBM -keyalg RSA
   -sigalg SHA256withRSA -keysize 2048 -validity jours -keystore
   key.jks -storepass mot de passe -keypass mot de passe
   ```

   Où :

   -dname CN=*nom de domaine complet*,**OU=Tivoli_Storage_Manager_for_VMware,O=IBM**
   : *nom de domaine complet* correspond au nom DNS ou au nom de domaine complet de l'ordinateur sur lequel l'interface graphique de Data Protection for VMware vSphere est installée.

   -validity *jours*
   : Période de validité du certificat.

   -storepass *mot de passe*
   : Mot de passe du fichier de clés. Assurez-vous de mémoriser ce mot de passe pour une utilisation ultérieure.

   -keypass *mot de passe*
   : Mot de passe de la clé privée pour le certificat. Ce mot de passe doit correspondre au mot de passe du fichier de clés.

5. Codez le mot de passe du fichier de clés à l'aide de l'outil **securityUtility**. Exécutez la commande ci-dessous.
   - Sous Linux : `/opt/tivoli/tsm/tdpvmware/common/webserver/bin/securityUtility encode`
   - Sous Windows : `C:\IBM\SpectrumProtect\webserver\bin\securityUtility.bat encode`

   Saisissez le mot de passe de votre fichier de clés lorsque vous y êtes invité, puis sauvegardez le résultat (par exemple, copiez-le dans le presse-papiers).
6. Ouvrez le fichier `bootstrap.properties` dans un éditeur et définissez la propriété `veProfile.keystore.pswd` sur la valeur codée générée à l'étape précédente. Le fichier `bootstrap.properties` se trouve à l'emplacement suivant :
   - Sous Linux : `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/`
   - Sous Windows : `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\`
7. Démarrez le service d'interface graphique de Data Protection for VMware vSphere.

Référence associée:

«Démarrage et exécution de services pour Data Protection for VMware», à la page 91

Création d'une demande de signature de certificat :

Après avoir accédé au fichier de clés, vous devez créer une demande de signature de certificat.

Procédure

Procédez comme suit pour créer une demande de signature de certificat.

1. A partir de la ligne de commande, accédez au répertoire où se trouve le fichier de clés.
   - Sous Linux : `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - Sous Windows : `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
2. Exécutez la commande suivante pour créer un certificat :

   ```
   keytool -genkeypair -alias maclé -dname
   CN=nom de domaine complet,OU=unité,O=organisation
   -keyalg RSA -sigalg SHA256withRSA
   -keysize 2048 -validity jours
   -keystore key.jks -storepass
   mot de passe -keypass mot de passe
   ```

   Où :

   -alias *maclé*
   : *maclé* correspond à l'alias unique qui identifie le certificat dans le fichier de clés. Il est renommé lorsque le certificat signé est reçu.

   -dname CN=*nom de domaine complet***,OU=***unité***,O=***organisation*
   : *nom de domaine complet* correspond au nom DNS ou au nom de domaine complet de l'ordinateur sur lequel l'Interface graphique de Data Protection for VMware vSphere est installée.

     Unité et *organisation* correspondent aux informations d'organisation qui sont requises par vos règles ou par l'autorité de certification.

   -validity *jours*
   : Période de validité du certificat.

   -storepass *mot de passe*
   : Mot de passe du fichier de clés. Si vous ne le connaissez pas ou que vous l'avez oublié, reportez-vous à la section «Accès au fichier de clés», à la page 67.

   -keypass *mot de passe*
   : Mot de passe de la clé privée pour le certificat. Ce mot de passe doit correspondre au mot de passe du fichier de clés.
3. Exécutez la commande suivante pour créer une demande de signature de certificat :

   ```
   keytool -certreq -alias maclé -file certreq.pem -keystore key.jks
   ```

   Où :

   -alias *maclé*
   : Alias de certificat généré à l'étape précédente.

   -file *certreq.pem*
   : Fichier où stocker la demande de signature de certificat.

Envoi de la demande de signature de certificat à l'autorité de certification :

Une fois que vous avez créé la demande de certificat (`certreq.pem`), vous devez l'envoyer à l'autorité de certification pour signature. Suivez les instructions spécifiques émises par l'autorité de certification.

Réception du certificat signé :

Une fois que vous avez obtenu le certificat signé de l'autorité de certification, vous devez recevoir le certificat dans le fichier de clés.

Procédure

Pour recevoir le certificat signé, procédez comme suit.

1. A partir de la ligne de commande, accédez au répertoire où se trouve le fichier de clés.
   - Sous Linux : `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - Sous Windows : `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
2. Copiez les fichiers reçus de l'autorité de certification à cet emplacement. Il s'agit du certificat racine de l'autorité de certification, des certificats intermédiaires de l'autorité de certification (le cas échéant) et du certificat signé pour l'interface graphique de Data Protection for VMware vSphere.
3. Arrêtez le service interface graphique de Data Protection for VMware vSphere.
4. Faites une copie de sauvegarde du fichier de clés (`key.jks`) en le renommant ou en le copiant à un autre emplacement.
5. Importez les certificats intermédiaires de l'autorité de certification (le cas échéant), à l'aide de la commande suivante. Lorsque vous êtes invité à faire confiance aux certificats, répondez *yes*. Répétez cette étape pour plusieurs certificats intermédiaires de l'autorité de certification, si nécessaire.

   ```
   keytool -importcert -alias certificat intermédiaire -file intermediate.pem
   -keystore key.jks -storepass mot de passe
   ```

   Où :

   -alias *certificat intermédiaire*
   Alias unique qui identifie le certificat dans le fichier de clés. Chaque certificat intermédiaire doit avoir un alias unique.

   -file *intermediate.pem*
   Fichier de certificat intermédiaire qui est obtenu de l'autorité de certification.

   -storepass *mot de passe*
   Mot de passe du fichier de clés.
6. Exécutez la commande suivante pour importer le certificat racine de l'autorité de certification. Lorsque vous êtes invité à faire confiance à ce certificat, répondez *yes*.

   ```
   keytool -importcert -alias certificat racine -file root.pem -keystore
   key.jks -storepass mot de passe
   ```

   Où :

   -alias *certificat racine*
   Alias unique qui identifie le certificat dans le fichier de clés.

-file *root.pem*
Fichier de certificat racine obtenu de l'autorité de certification.

-storepass *mot de passe*
Mot de passe du fichier de clés.

7. Exécutez la commande suivante pour importer le certificat signé :

```
keytool -importcert -alias maclé -file signedcert.pem -keystore
key.jks -storepass mot de passe
```

Où :

-alias *maclé*
Alias du certificat signé. L'alias doit être le même que celui utilisé lorsque vous avez généré la demande de signature de certificat.

-file *signedcert.pem*
Fichier de certificat signé reçu de l'autorité de certification.

-storepass *mot de passe*
Mot de passe du fichier de clés.

8. Supprimez le certificat existant qui contient l'alias `vekey` :

```
keytool -delete -alias vekey -keystore key.jks -storepass mot de passe
```

Où `-storepass` *mot de passe* correspond au mot de passe du fichier de clés.

9. Renommez le certificat signé en `vekey` :

```
keytool -changealias -alias maclé -destalias vekey -keystore
key.jks -storepass mot de passe
```

Où :

-alias *maclé*
Alias du certificat signé.

-storepass *mot de passe*
Mot de passe du fichier de clés.

10. Démarrez le service d'interface graphique de Data Protection for VMware vSphere.

Référence associée:

«Démarrage et exécution de services pour Data Protection for VMware», à la page 91

Exigences en termes de privilèges utilisateur du serveur VMware vCenter

Des privilèges du serveur VMware vCenter sont nécessaires pour exécuter certaines opérations de Data Protection for VMware.

Privilèges du serveur vCenter requis pour protéger les centres de données VMware à l'aide de la vue du navigateur web pour l'Interface graphique de Data Protection for VMware vSphere

L'ID utilisateur du serveur vCenter utilisé pour la connexion à la vue du navigateur pour l'Interface graphique de Data Protection for VMware vSphere

doit avoir des privilèges VMware suffisants pour voir le contenu d'un centre de données géré par l'interface graphique.

Par exemple, un environnement VMware vSphere contient cinq centres de données. Un utilisateur, «jenn», possède des privilèges suffisants pour seulement deux de ces centres de données. En conséquence, seuls ces deux centres de données sont visibles par «jenn» dans les vues. Les trois autres centres de données (pour lesquels «jenn» ne possède pas de privilèges) ne sont pas visibles par l'utilisateur «jenn».

Le serveur VMware vCenter définit collectivement un ensemble de privilèges en tant que rôle. Un rôle s'applique à un objet pour un utilisateur ou un groupe spécifié pour créer un privilège. A partir du client Web VMware vSphere, vous devez créer un rôle avec un ensemble de privilèges. Pour créer un rôle de serveur vCenter pour des opérations de sauvegarde et de restauration, utilisez la fonction **Add a Role** du client WMware vSphere.

Si vous souhaitez propager les privilèges à tous les centres de données au sein de vCenter, spécifiez le serveur vCenter et cochez la case `Propagate to children`. Vous pouvez aussi limiter les droits si vous affectez le rôle aux centres de données requis uniquement à l'aide de la case à cocher `Propagate to children` sélectionnée. L'application pour l'interface graphique du navigateur s'effectue au niveau du centre de données.

L'exemple ci-après montre comment contrôler l'accès aux centres de données pour deux groupes d'utilisateurs VMware. Commencez par créer un rôle qui contient tous les privilèges définis dans la note technique 7047438. Les privilèges utilisés dans cet exemple sont identifiés par le rôle «TDPVMwareManage». Le groupe 1 nécessite un accès afin de restaurer des machines virtuelles pour les centres de données `Primary1_DC` et `Primary2_DC`. Le groupe 2 nécessite un accès afin de gérer des machines virtuelles pour les centres de données `Secondary1_DC` et `Secondary2_DC`.

Pour le groupe 1, affectez le rôle «TDPVMwareManage» aux centres de données `Primary1_DC` et `Primary2_DC`. Pour le groupe 2, affectez le rôle «TDPVMwareManage» aux centres de données `Secondary1_DC` et `Secondary2_DC`.

Les utilisateurs de chaque groupe d'utilisateurs VMware peuvent utiliser l'interface graphique de Data Protection for VMware pour gérer des machines virtuelles dans leurs centres de données respectifs uniquement.

Conseil : Lorsque vous créez un rôle, vous devez envisager de lui ajouter des privilèges supplémentaires dont vous aurez peut-être besoin pour effectuer d'autres tâches sur des objets.

Privilèges du serveur vCenter requis pour utiliser le dispositif de transfert de données

Le dispositif de transfert de données IBM Spectrum Protect qui est installé sur le serveur de stockage vStorage (noeud de dispositif de transfert de données) nécessite les options `VMCUser` et `VMCPw`. L'option `VMCUser` spécifie l'ID utilisateur du serveur vCenter ou ESX que vous souhaitez sauvegarder, restaurer ou interroger. Les privilèges requis affectés à cet ID utilisateur (`VMCUser`) garantissent que le client peut exécuter des opérations sur la machine virtuelle et dans l'environnement VMware. Cet ID utilisateur doit disposer des privilèges décrits dans la note technique ci-dessus.

Pour créer un rôle de serveur vCenter pour des opérations de sauvegarde et de restauration, utilisez la fonction **Add a Role** du client WMware vSphere. Vous

devez sélectionner l'option `Propagate to children` lorsque vous ajoutez des privilèges pour cet ID utilisateur (`VMCUser`). De plus, vous devez envisager d'ajouter d'autres privilèges à ce rôle pour des tâches autres que la sauvegarde et la restauration. Pour l'option `VMCUser`, la mise en application s'effectue au niveau de l'objet sommet.

Privilèges du serveur vCenter requis pour protéger les centres de données VMware à l'aide de la vue du Plug-in client IBM Spectrum Protect vSphere pour l'Interface graphique de Data Protection for VMware vSphere

Le Plug-in client IBM Spectrum Protect vSphere nécessite un ensemble de privilèges distinct des privilèges qui sont nécessaires pour se connecter à l'interface graphique.

Lors de l'installation, les privilèges personnalisés suivants sont créés pour le Plug-in client IBM Spectrum Protect vSphere :

- **Centre de données** > **IBM Data Protection**
- **Global** > **Configuration d'IBM Data Protection**

Les privilèges personnalisés qui sont requis pour le Plug-in client IBM Spectrum Protect vSphere sont enregistrés en tant qu'extension distincte. La clé d'extension des privilèges est `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

Ces privilèges permettent à l'administrateur VMware d'activer et de désactiver l'accès au contenu du Plug-in client IBM Spectrum Protect vSphere. Seuls les utilisateurs dotés de ces privilèges personnalisés sur l'objet VMware requis peuvent accéder au contenu du Plug-in client IBM Spectrum Protect vSphere. Un Plug-in client IBM Spectrum Protect vSphere est enregistré pour chaque serveur vCenter et partagé par tous les hôtes d'interface graphique qui sont configurés pour prendre en charge le serveur vCenter.

A partir du client Web VMware vSphere, vous devez créer un rôle pour les utilisateurs qui peuvent exécuter des fonctions de protection des données des machines virtuelles à l'aide du Plug-in client IBM Spectrum Protect vSphere. Pour ce rôle, outre les privilèges de rôle administrateur de machine virtuelle standard requis par le client Web, vous devez spécifier le privilège **Centre de données** > **IBM Data Protection**. Pour chaque centre de données, affectez ce rôle à chaque utilisateur ou groupe d'utilisateurs auquel vous souhaitez accorder le droit de gérer des machines virtuelles.

Le privilège **Global** > **IBM Data Protection** est requis pour l'utilisateur au niveau de vCenter. Ce privilège permet à l'utilisateur de gérer, d'éditer ou de supprimer la connexion entre le serveur vCenter et le serveur Web de l'interface graphique de Data Protection for VMware vSphere. Affectez ce privilège aux administrateurs qui maîtrisent l'interface graphique de Data Protection for VMware vSphere qui protège leur serveur vCenter respectif. Gérez vos connexions au Plug-in client IBM Spectrum Protect vSphere sur la page Connections de l'extension.

L'exemple ci-après montre comment contrôler l'accès aux centres de données pour deux groupes d'utilisateurs. Le groupe 1 nécessite un accès afin de gérer des machines virtuelles pour les centres de données `NewYork _DC` et `Boston_DC`. Le groupe 2 nécessite un accès afin de gérer des machines virtuelles pour les centres de données `LosAngeles_DC` et `SanFranciso_DC`.

A partir du client VMware vSphere, créez par exemple le rôle «IBMDataProtectManage», affectez les privilèges de rôle administrateur de machine virtuelle standard, ainsi que le privilège **Datacenter** > **IBM Data Protection**.

Pour le groupe 1, affectez le rôle «IBMDataProtectManage» aux centres de données `NewYork _DC` et `Boston_DC`. Pour le groupe 2, affectez le rôle «IBMDataProtectManage» aux centres de données `LosAngeles_DC` et `SanFranciso_DC`.

Les utilisateurs de chaque groupe peuvent utiliser le Plug-in client IBM Spectrum Protect vSphere dans le client Web vSphere pour gérer des machines virtuelles dans leurs centres de données respectifs uniquement.

Problèmes liés à des droits insuffisants

Lorsque l'utilisateur du navigateur web ne dispose pas de droits suffisants pour un centre de données, l'accès à la vue est bloqué. Le message d'erreur GVM2013E est généré pour informer l'utilisateur qu'il ne dispose pas des droits suffisants pour accéder aux centres de données gérés. D'autres nouveaux messages sont également disponibles pour informer les utilisateurs des problèmes liés aux droits insuffisants. Pour résoudre les problèmes liés aux droits, vérifiez que le rôle utilisateur est bien configuré comme décrit dans les sections précédentes. Le rôle utilisateur doit disposer de tous les privilèges identifiés dans le tableau Privilèges requis pour l'ID utilisateur du serveur VCenter et le dispositif de transfert de données et ces privilèges doivent être appliqués au niveau du centre de données à l'aide de la case `propagate to children`.

Lorsque l'utilisateur du Plug-in client IBM Spectrum Protect vSphere ne dispose pas de droits suffisants pour accéder à un centre de données, les fonctions de protection des données du centre ainsi que son contenu ne sont pas accessibles à l'extension.

Lorsque l'ID utilisateur de IBM Spectrum Protect (spécifié par l'option `VMCUser`) ne dispose pas des droits suffisants pour une opération de sauvegarde et de restauration, le message suivant s'affiche :

```
ANS9365E Erreur d'interface de programme d'application VMware vStorage.
"Cette opération n'est pas autorisée."
```

Lorsque l'ID utilisateur de IBM Spectrum Protect ne dispose pas des droits suffisants pour afficher une machine, les messages suivants s'affichent :

```
Commande de sauvegarde de machine virtuelle lancée.
Nombre total de machines virtuelles à traiter : 1
ANS4155E Machine virtuelle 'tango' introuvable sur le serveur VMware.
ANS4148E La sauvegarde intégrale de la machine virtuelle 'foxtrot' a échoué
avec le code retour 4390
```

Pour plus d'informations sur l'utilisation des privilèges, voir la note **vCenter Server privileges required for the Data Protection for VMware vSphere GUI and data mover**.

Pour extraire des informations de journal via le serveur VMware Virtual Center pour plus d'informations sur les problèmes liés aux droits d'accès, procédez comme suit.

1. Dans vCenter Server Settings, sélectionnez **Logging Options** et affectez la valeur **Trivia (Trivia)** au paramètre **vCenter Logging**.
2. Recréez l'erreur liée aux droits d'accès.

3. Restaurez la valeur précédente du paramètre **vCenter Logging** pour éviter qu'un nombre excessif de données de journal ne soit collecté.
4. Dans System Logs, recherchez la chaîne `NoPermission` dans le journal de serveur vCenter le plus récent (`vpxd-wxyz.log`). Par exemple :

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
   vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Throw: vim.fault.NoPermission
   ```

   Ce message de journal indique que l'ID utilisateur ne possédait pas suffisamment de droits pour créer une image instantanée (`createSnapshot`).

Rôles utilisateur de l'Interface graphique de Data Protection for VMware vSphere

La disponibilité des fonctions de l'Interface graphique de Data Protection for VMware vSphere dépend du niveau d'autorisation affecté à votre ID administrateur dans IBM Spectrum Protect.

L'ID d'administrateur doit être identique au nom du noeud. Dans les anciennes versions du produit, la commande **REGISTER NODE** créait automatiquement un ID d'administration au nom identique à celui du noeud. A compter de la version 8.1 de IBM Spectrum Protect, la commande **REGISTER NODE** ne crée plus automatiquement d'ID utilisateur d'administration identique au nom du noeud.

Lors de l'enregistrement d'un nouveau noeud, l'administrateur du serveur IBM Spectrum Protect doit spécifier le paramètre `userid` avec la commande de serveur **REGISTER NODE** :

```
REGISTER NODE nom_noeud mot_de_passe userid=id_utilisateur
```

Le nom du noeud et l'ID utilisateur administratif doit être identiques. Par exemple :

```
REGISTER NODE noeud_a m0tdep4sse userid=noeud_a
```

Par défaut, le noeud a l'autorité du propriétaire du client.

Les tâches que vous pouvez effectuer à l'aide de l'Interface graphique de Data Protection for VMware vSphere dépendent de la classe de privilèges affectée à l'ID administrateur.

Lorsque l'ID administrateur ne dispose pas de privilèges de domaine de règles non restreints, vous ne pouvez pas enregistrer de nouveaux noeuds ou définir leur relation proxy sur le serveur IBM Spectrum Protect. Si vous n'entrez pas un ID administrateur, un script macro est créé afin de pouvoir l'exécuter sur le serveur IBM Spectrum Protect.

Un ID administrateur IBM Spectrum Protect est obligatoire lors de la configuration de l'Interface graphique de Data Protection for VMware vSphere. Le tableau suivant répertorie les fonctions disponibles en fonction de la classe de privilèges affectée à cet ID :

- Une valeur Oui indique une fonction disponible pour le rôle utilisateur.
- Une valeur Non indique une fonction qui est disponible pour le rôle utilisateur.

Pour afficher votre rôle actuel pour l'Interface graphique de Data Protection for VMware vSphere, survolez le curseur sur votre ID utilisateur dans la barre de navigation.

Tableau 11. Fonctions disponibles selon les privilèges d'ID administrateur IBM Spectrum Protect

	Opérateur	**Opérateur avec droits de création de rapports**	**Administrateur avec droits limités**	**Administrateur**
Récapitulatif	Exécuter la sauvegarde et la restauration maintenant	Opérateur plus production de rapports	Opérateur plus production de rapports et opérations de planification pour les domaines de règles répertoriés	Tous les rôles, y compris la configuration initiale
IBM Spectrum Protect ID Admin Classe de privilèges	Néant	L'une des classes de privilèges suivantes : • Stockage • Opérateur • Analyste	Règle (restreint) ou l'une des classes de privilèges suivantes: • Stockage • Opérateur • Analyste	Règle (non restreinte) ou système
		Onglet Sauvegarder		
Gérer **l'exécution** des tâches de sauvegarde maintenant	Oui	Oui	Oui	Oui
Gérer **la planification** des tâches de sauvegarde maintenant	Non[1]	Non[1]	Oui, dans les domaines de règles	Oui
Afficher **l'exécution** des tâches de sauvegarde	Oui	Oui	Oui	Oui
Afficher des tâches de sauvegarde **Planifiées**	Non	Oui	Oui	Oui
Supprimer une tâche de sauvegarde **Planifiée**	Non	Non	Oui dans les domaines de règles	Oui
		Onglet Restaurer		
Exécution d'une tâche de **Restauration**	Oui	Oui	Oui	Oui
		Onglet Rapports		
Evénements	Non	Oui	Oui	Oui
Tâches récentes	Oui	Oui	Oui	Oui
Etat de sauvegarde	Non	Oui	Oui	Oui
Protection d'application	Non	Oui	Oui	Oui
Occupation du centre de données	Non	Oui	Oui	Oui

Tableau 11. Fonctions disponibles selon les privilèges d'ID administrateur IBM Spectrum Protect (suite)

	Opérateur	Opérateur avec droits de création de rapports	Administrateur avec droits limités	Administrateur
		Onglet Configuration		
Enregistrement de noeud (Etat de configuration -> **Exécution de l'assistant de configuration**)	Non	Non	Non[2]	Oui
Modifier les données d'identification d'ID administrateur IBM Spectrum Protect (Etat de la configuration -> **Modifier la configuration**)	Oui	Oui	Oui	Oui
Modifier le mot de passe du noeud VMCLI (Etat de la configuration -> **Editer la configuration**)	Non	Non	Oui	Oui
Modifier les domaines d'interface graphique (Etat de la configuration -> **Editer la configuration**)	Oui[3]	Oui[3]	Oui[3]	Oui
Modifier les noeuds de transfert de données (Etat de la configuration -> **Editer la configuration**)	Non	Non	Non[2]	Oui
Modifier les noeuds proxy de montage (Etat de la configuration -> **Editer la configuration**)	Non	Non	Non[2]	Oui

1. Vous ne pouvez pas enregistrer le noeud, car un domaine de règles à droits illimités est requis.
2. Vous pouvez ajouter ou supprimer des centres de données VMware et enregistrer des noeuds de centre de données.

Pour afficher le niveau d'autorisation de l'ID administrateur IBM Spectrum Protect et le rôle d'Interface graphique de Data Protection for VMware vSphere correspondant :

1. Accédez à la fenêtre Configuration.
2. Cliquez sur **Modifier la configuration**.
3. Les informations recherchées s'affichent dans la page Données d'identification du serveur Spectrum Protect.

Important :

- Si le niveau d'autorisation d'un ID administrateur dans IBM Spectrum Protect change sur le serveur IBM Spectrum Protect, l'Interface graphique de Data Protection for VMware vSphere doit être redémarrée pour refléter ce changement.
- Lorsque vous modifiez le Rôle utilisateur, vous devez cliquer sur **OK** afin d'enregistrer vos changements avant d'aller sur une autre page de Paramètres de configuration ou d'essayer un autre changement de configuration. Autrement, le changement de Rôle utilisateur ne prend pas effet.

Clés d'enregistrement de l'interface graphique de Data Protection for VMware

Selon les options que vous sélectionnez lors de l'installation, vous pouvez accéder à l'interface graphique de Data Protection for VMware via différentes méthodes. Des clés d'enregistrement sont créées pour les intefaces graphiques de Data Protection for VMware.

Le terme «Interface graphique de Data Protection for VMware» se réfère aux interfaces graphiques suivantes :

- Interface graphique de Data Protection for VMware vSphere accessible dans un navigateur Web
- Le Plug-in client IBM Spectrum Protect vSphere dans l'interface graphique client Web vSphere

La clé d'enregistrement du Plug-in client IBM Spectrum Protect vSphere est `com.ibm.tsm.tdpvmware.IBMDataProtection`. Cette clé est enregistrée lorsque vous cochez la case **Register the vSphere Web Client extension** lors de l'installation. Une seule instance du Plug-in client IBM Spectrum Protect vSphere est enregistrée par serveur vCenter.

Une clé d'enregistrement n'est pas créée pour l'Interface graphique de Data Protection for VMware vSphere accessible dans un navigateur Web.

Pour afficher la clé d'enregistrement, connectez-vous au navigateur d'objets gérés par VMware (MOB). Une fois connecté au navigateur MOB, accédez à **Content→Extension Manager** pour voir les clés d'enregistrement.

Configuration de l'interface graphique de Recovery Agent

Cette section explique comment configurer l'interface graphique de Recovery Agent dans le cadre des opérations de montage, de restauration de fichier et de restauration instantanée.

Avant de commencer

Ces tâches de configuration doivent être exécutées avant toute tentative d'exécution d'une opération dans l'interface graphique de Recovery Agent.

Important : Des informations sur l'exécution de ces tâches depuis l'interface graphique de Recovery Agent sont disponibles dans l'aide en ligne installée avec l'interface graphique. Cliquez sur **Aide** dans l'une des fenêtres de l'interface pour ouvrir l'aide en ligne et obtenir de l'assistance.

Procédure

1. Connectez-vous au système sur lequel vous souhaitez restaurer des fichiers. Recovery Agent doit être installé sur le système.
2. Cliquez sur **Sélectionner un serveur TSM** dans l'interface graphique de Recovery Agent pour vous connecter à un serveur IBM Spectrum Protect. Lorsque Recovery Agent est installé sur le même système que l'Interface graphique de Data Protection for VMware vSphere et que les applications ont été configurées à l'aide de l'assistant de configuration de l'Interface graphique de Data Protection for VMware vSphere, les conditions suivantes sont réunies :
   - Le noeud de dispositif de transfert de données et le serveur IBM Spectrum Protect sont renseignés dans la zone Serveur TSM de Recovery Agent.
   - Les zones suivantes du panneau Informations sur le serveur TSM sont remplies :
     - **Noeud d'authentification** contient la liste des noeuds de dispositif de transfert de données disponibles.
     - **Noeud cible** contient la liste des noeuds de centre de données disponibles pour le noeud de dispositif de transfert de données sélectionné.

   Lorsqu'un seul noeud de dispositif de transfert de données a été défini en local à l'aide de l'assistant de configuration, Recovery Agent l'utilise pour s'authentifier lors de son démarrage.Recovery Agent se souvient du dernier nom de noeud qui s'est connecté au serveur IBM Spectrum Protect. Si l'option **Utiliser le mot de passe pour générer l'accès** est sélectionnée pour ce noeud (le dernier à se connecter), Recovery Agent utilise ces données d'identification pour se connecter au serveur IBM Spectrum Protect lors du démarrage. Si aucune connexion précédente au serveur IBM Spectrum Protect n'a été effectuée et si un seul noeud de dispositif de transfert de données et un noeud de centre de données sont configurés avec l'assistant, Recovery Agent utilise ces informations d'identification et de connexion pour se connecter au serveur IBM Spectrum Protect au démarrage.

   Spécifiez les options suivantes :

   Adresse du serveur
   Entrez l'adresse IP ou le nom d'hôte de IBM Spectrum Protect.

   Port du serveur
   Entrez le numéro de port qui est utilisé pour la communication TCP/IP avec le serveur. Le numéro de port par défaut est 1500.

   Méthode d'accès au noeud :

   Asnodename
   Cette option permet d'utiliser un noeud proxy pour accéder aux sauvegardes de machine virtuelle du noeud cible. Le noeud proxy est un noeud disposant des droits proxy afin d'effectuer des opérations au nom du noeud cible.

   L'administrateur IBM Spectrum Protect utilise généralement la commande `grant proxynode` pour créer la relation proxy entre deux noeuds existants.

   Si vous sélectionnez cette option, procédez comme suit :

a. Entrez le nom du noeud cible (le noeud sur lequel les sauvegardes de machine virtuelle se trouvent) dans la zone **Noeud cible**.
b. Entrez le nom du noeud proxy dans la zone **Noeud d'authentification**.
c. Entrez le mot de passe du noeud proxy dans la zone **Mot de passe**.
d. Cliquez sur **OK** pour sauvegarder ces paramètres et quitter la boîte de dialogue d'informations IBM Spectrum Protect.

Lorsque vous utilisez cette méthode, l'utilisateur de Recovery Agent connaît uniquement le mot de passe du noeud proxy. Le mot de passe du noeud cible est protégé.

Fromnode
Cette option permet d'utiliser un noeud avec un accès limité uniquement aux données d'image instantanée de machines virtuelles spécifiques dans le noeud cible.

Ce noeud obtient généralement l'accès au noeud cible propriétaire des sauvegardes de machine virtuelle à l'aide de la commande `set access` :

```
set access backup -TYPE=VM vmdisplayname mountnodename
```

Par exemple, cette commande donne au noeud `myMountNode` les droits d'accès pour la restauration des fichiers de la machine virtuelle `myTestVM` :

```
set access backup -TYPE=VM myTestVM myMountNode
```

Si vous sélectionnez cette option, procédez comme suit :

a. Entrez le nom du noeud cible (le noeud sur lequel les sauvegardes de machine virtuelle se trouvent) dans la zone **Noeud cible**.
b. Entrez le nom du noeud ayant un accès limité dans la zone **Noeud d'authentification**.
c. Entrez le mot de passe du noeud ayant un accès limité dans la zone **Mot de passe**.
d. Cliquez sur **OK** pour sauvegarder ces paramètres et quitter la boîte de dialogue d'informations IBM Spectrum Protect.

Lorsque vous utilisez cette méthode, vous pouvez accéder à la liste complète des machines virtuelles sauvegardées. Toutefois, vous pouvez uniquement restaurer les machines virtuelles pour lesquelles le noeud a obtenu l'accès. En outre, les données d'image instantanée ne sont pas protégées de l'expiration sur le serveur. Il en résulte que la restauration instantanée n'est pas prise en charge dans cette méthode.

Direct Sélectionnez cette option pour vous authentifier directement auprès du noeud cible (le noeud où se situent les sauvegardes de machine virtuelle).

Si vous sélectionnez cette option, procédez comme suit :

a. Entrez le nom du noeud cible (le noeud où se situent les sauvegardes de machine virtuelle) dans la zone **Noeud d'authentification**.
b. Entrez le mot de passe du noeud cible dans la zone **Mot de passe**.
c. Cliquez sur **OK** pour sauvegarder ces paramètres et quitter la boîte de dialogue d'informations IBM Spectrum Protect.

Utiliser le mot de passe pour générer l'accès
Lorsque cette option est sélectionnée et que la zone de mot de passe est

vide, Recovery Agent s'authentifie avec un mot de passe existant qui est stocké dans le registre. Si l'option n'est pas sélectionnée, vous devez entrer manuellement le mot de passe.

Pour utiliser cette option, vous devez commencer par définir manuellement un mot de passe initial pour le noeud auquel elle s'applique. Vous devez spécifier ce mot de passe lorsque vous vous connectez pour la première fois au noeud IBM Spectrum Protect en entrant le mot de passe figurant dans la zone **Mot de passe** et en cochant la case **Utiliser le mot de passe pour générer l'accès**.

Toutefois, lorsque vous utilisez le noeud de dispositif de transfert de données locales comme **Noeud d'authentification**, le mot de passe peut déjà être stocké dans le registre. Par conséquent, cochez la case **Utiliser le mot de passe pour générer l'accès** et n'entrez pas de mot de passe.

Recovery Agent demande au serveur spécifié la liste des machines virtuelles protégées et affiche cette liste.

3. Définissez les options de montage, sauvegarde et restauration suivantes en cliquant sur **Paramètres** :

Cache en écriture du volume virtuel
L'agent Recovery Agent qui s'exécute sur l'hôte proxy de sauvegarde Windows sauvegarde les modifications créées lors de la restauration instantanée et du montage. Ces modifications sont enregistrées sur un volume virtuel du cache en écriture. Par défaut, le cache en écriture est activé et spécifie le chemin `C:\ProgramData\Tivoli\TSM\TDPVMware\mount\` et la taille maximale du cache est de 90 % de l'espace disponible pour le dossier sélectionné. Pour éviter toute saturation du système, remplacez le cache en écriture par un chemin se trouvant sur un autre volume que le volume système.

Dossier de fichiers temporaires
Indiquez l'emplacement d'enregistrement des modifications de données. Le cache en écriture doit se trouver sur une unité locale et ne peut pas être défini sur un chemin d'accès à un dossier partagé. Si le cache d'écriture est désactivé ou plein, aucune session de restauration instantanée ou de montage ne pourra être démarrée.

Taille de la mémoire cache de l'image instantanée
Indiquez la taille du cache en écriture. La taille maximale admise du cache est égale à 90 % de l'espace disponible pour le dossier sélectionné.

Restriction : Pour éviter toute interruption lors de la restauration, excluez le chemin d'accès au cache en écriture de tous les paramètres de protection de vos logiciels antivirus.

Accès aux données
Indiquez le type de données auxquelles vous souhaitez accéder. Si vous utilisez une unité hors ligne (comme une bande magnétique ou une bandothèque virtuelle), vous devez indiquer le type de données correspondant.

Type de stockage
Spécifiez l'une des unités de stockage suivantes à partir de laquelle monter l'instantané :

Disque/Fichier
Cette option permet d'indiquer que l'image instantanée est montée à partir d'un disque ou d'un fichier. Il s'agit de l'unité par défaut.

Bande Cette option permet d'indiquer que l'image instantanée est montée à partir d'un pool de stockage de bandes. Lorsque cette option est sélectionnée, il n'est pas possible de monter plusieurs instantanés ou d'exécuter une opération de restauration instantanée.

VTL L'instantané est monté à partir d'une bandothèque virtuelle hors ligne. Il est possible d'exécuter plusieurs sessions de montage simultanées sur la même bandothèque virtuelle.

Remarque : En cas de modification du type de stockage, il est nécessaire de redémarrer le service pour que les modifications prennent effet.

Désactiver la protection d'expiration
Lors d'une opération de montage, l'image instantanée située sur le serveur IBM Spectrum Protect est verrouillée pour éviter d'expirer en cours d'opération. Un dépassement du délai d'expiration peut se produire lorsqu'une autre image instantanée est ajoutée à la séquence de l'image instantanée montée. Cette valeur indique si la protection du délai d'expiration doit être désactivée lors de l'opération de montage.

- Pour empêcher l'expiration d'une image instantanée, laissez cette option non sélectionnée. L'image instantanée du serveur IBM Spectrum Protect est verrouillée et ne peut pas expirer durant l'opération de montage.
- Pour désactiver le mode anti-expiration, sélectionnez cette option. Cette option est sélectionnée par défaut. L'image instantanée du serveur IBM Spectrum Protect n'est pas verrouillée et n'est pas protégée contre l'expiration lors de l'opération de montage. Par conséquent, elle peut expirer durant l'opération de montage. Cette expiration peut causer des résultats inattendus et avoir un impact négatif sur le point de montage. Par exemple, le point de montage peut devenir inutilisable ou contenir des erreurs. Toutefois, l'expiration n'affecte pas la copie active en cours. La copie active ne peut pas expirer lors d'une opération.

  Lorsque l'image instantanée se trouve sur un serveur de réplication cible, elle ne peut pas être verrouillée car elle se trouve en mode de lecture seule. Toute tentative de verrouillage par le serveur entraîne l'échec de l'opération de montage. Pour éviter les tentatives de verrouillage et ce type de pannes, désactivez la protection anti-expiration en sélectionnant cette option.

Taille de lecture anticipée (en blocs de 16 ko)
Indiquez le nombre de blocs de données supplémentaires récupérés à partir de l'unité de stockage suite à une demande de lecture envoyée sur un seul bloc. Les valeurs par défaut sont les suivantes :

- Disque ou fichier : 64

- Bande : 1024
- Bandothèque virtuelle : 64

La valeur maximum pour tout type d'unité est 1024.

Taille du cache de lecture anticipée (en blocs)
Indiquez la taille du cache où les blocs de données supplémentaires sont stockés. Les valeurs par défaut sont les suivantes :

- Disque ou fichier : 10000
- Bande : 75000
- Bandothèque virtuelle : 10000

Chaque image instantanée disposant de son cache, n'oubliez pas de prévoir le nombre d'images instantanées montées ou restaurées simultanément. La taille cumulée du cache ne peut pas dépasser 75 000 blocs.

Dépassement du délai d'attente du pilote (secondes)
Cette valeur indique la durée du traitement des demandes de données à partir du pilote du système de fichiers. Si le traitement ne se termine pas à l'heure, la demande est annulée et une erreur est renvoyée au pilote du système de fichiers. Augmentez cette valeur en cas de délais d'attente. Ceux-ci peuvent par exemple se produire lorsque le réseau est lent, que le périphérique de stockage est occupé ou que plusieurs sessions de montage ou de restauration instantanée sont en cours de traitement. Les valeurs par défaut sont les suivantes :

- Disque ou fichier : 60
- Bande : 180
- Bandothèque virtuelle : 60

Cliquez sur **OK** pour sauvegarder les modifications et quitter les **Paramètres**.

4. Vérifiez que chaque noeud de serveur IBM Spectrum Protect (spécifié avec les options `Asnodename` et `Fromnode`) permet la suppression des sauvegardes. L'agent Recovery Agent crée des objets temporaires inutilisés lors des opérations. L'option du serveur `BACKDELete=Yes` permet la suppression de ces objets afin qu'ils ne s'accumulent pas dans le noeud.
   a. Connectez-vous au serveur IBM Spectrum Protect et démarrez une session client d'administration en mode de ligne de commande :
      ```
      dsmadmc -id=admin -password=admin -dataonly=yes
      ```
   b. Entrez la commande suivante :
      ```
      Query Node <nodename> Format=Detailed
      ```
      Vérifiez que le résultat de la commande de chaque noeud comprend l'instruction suivante :
      ```
      Suppression de sauvegarde autorisée ? : Oui
      ```
      Si cette instruction n'est pas incluse, mettez à jour chaque noeud à l'aide de la commande suivante :
      ```
      UPDate Node <nodename> BACKDELete=Yes
      ```

Exécutez à nouveau la commande `Query Node` pour chaque noeud afin de vérifier que chaque noeud autorise la suppression des sauvegardes.

5. Lorsque Recovery Agent est utilisé dans un réseau iSCSI et qu'il n'utilise pas de dispositif de transfert de données, accédez au fichier `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf file` et spécifiez la balise `[IMOUNT]` et le paramètre **`Target IP`** :

```
[IMOUNT config]
Target IP=<adresse IP de la carte réseau sur le système
exposant les cibles iSCSI.>
```

Par exemple :

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

Après avoir ajouté ou changé le paramètre Target IP, redémarrez l'interface graphique de l'agent de récupération ou son interface CLI.

Activation de la communication sécurisée entre Recovery Agent et le serveur IBM Spectrum Protect

Si le serveur IBM Spectrum Protect est configuré pour utiliser le protocole SSL (Secure Sockets Layer) ou TLS (Transport Layer Security), vous pouvez faire en sorte que Recovery Agent communique avec le serveur par ce protocole.

Avant de commencer

Tenez compte des points suivants avant de commencer à configurer l'agent pour qu'il communique de façon sécurisée avec le serveur :

- Chaque serveur à même de communiquer par SSL doit avoir un certificat qui lui est propre. Ce certificat peut être de l'un des types suivants :
  - Un certificat autosigné par le serveur.
  - Un certificat émis par le biais d'un certificat d'autorité de certification (CA) tierce. Le certificat de CA peut provenir d'une société telle que Symantec ou Thawte. Il peut aussi s'agir d'un certificat "maison", tenu à jour et utilisé en interne par votre société.
- Pour des questions de performance, vous ne devez utiliser SSL ou TLS que pour les sessions qui ont véritablement besoin d'être sécurisées. Voyez s'il est judicieux d'ajouter davantage de ressources processeur au système du serveur afin de faire face à la demande accrue.
- Pour qu'un client puisse se connecter à un serveur en utilisant le protocole TLS version 1.2, l'algorithme de signature du certificat doit être SHA-1 ou version ultérieure. En cas d'utilisation d'un certificat autosigné pour communiquer avec un serveur utilisant TLS V1.2, le certificat utilisé doit être celui du fichier `cert256.arm`. Votre administrateur IBM Spectrum Protect pourrait avoir besoin de changer le certificat par défaut sur le serveur.
- Pour désactiver les protocoles de sécurité moins sûrs que TLS 1.2, ajoutez l'option **`SSLDISABLELEGACYtls yes`** au fichier `C:\windows\system32\fb.opt` ou `C:\Windows\SysWOW64\fb.opt`. Les versions 1.2 et ultérieures de TLS aident à parer les attaques des programmes malveillants.

Activation de la communication sécurisée en utilisant un certificat autosigné sur le serveur IBM Spectrum Protect

Si le serveur IBM Spectrum Protect utilise un certificat autosigné, vous devez en obtenir une copie auprès de l'administrateur du serveur et configurer Recovery Agent de sorte qu'il communique avec le serveur en utilisant le protocole SSL ou TLS.

Pourquoi et quand exécuter cette tâche

Chaque serveur génère son propre certificat. Les serveurs des versions 6.3 et ultérieures génèrent un fichier nommé `cert256.arm` s'ils utilisent TLS version 1.2 ou ultérieure, ou `cert.arm` s'ils utilisent une version plus ancienne de SSL ou TLS. Les serveurs des versions plus anciennes (antérieures à la 6.3) génèrent un fichier nommé `cert.arm` quelle que soit la version de protocole utilisée. Vous devez choisir le certificat défini par défaut sur le serveur.

Le fichier du certificat est stocké sur le poste de travail du serveur, dans le répertoire d'instance du serveur. Par exemple, `C:\IBM\tivoli\tsm\server\bin\cert256.arm`. Si le fichier du certificat n'existe pas, il est créé au redémarrage du serveur avec ce jeu d'options.

Procédure

Pour permettre à l'agent de récupération de communiquer avec le serveur par SSL ou TLS avec un certificat autosigné :

1. Ajoutez à la variable d'environnement PATH du client le chemin des binaires du GSKit ainsi que celui des bibliothèques. Par exemple :

   ```
   set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
       C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. S'il s'agit de la première configuration de SSL ou TLS sur le client, vous devez créer sa base de données de clés locale, dsmcert.kdb. A partir du répertoire `C:\Windows\SysWOW64`, lancez la commande **gsk8capicmd_64** comme dans l'exemple suivant :

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw mot_de_passe -stash
   ```

   Le mot de passe que vous fournissez sert à chiffrer la base de données de clés. Le mot de passe est automatiquement stocké sous forme chiffrée dans le fichier de dissimulation (dsmcert.sth). Ce fichier est utilisé par le client pour obtenir le mot de passe de la base de données de clés.

3. Obtenez le certificat autosigné du serveur.
4. Importez le certificat dans la base de données dsmcert.kdb. Le certificat doit être importé dans la base de données de clés de chaque client. A partir du répertoire `C:\Windows\SysWOW64`, lancez la commande **gsk8capicmd_64** comme dans l'exemple suivant :

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Clé autosignée du serveur nom_serveur"
   -file chemin_certificat -format ascii -trust enable
   ```

   Plusieurs certificats de différents serveurs peuvent être ajoutés à la base de données dsmcert.kdb afin que le client puisse se connecter à ces serveurs. Chaque certificat doit avoir son propre label. Utilisez un nom significatif pour chacun.

Important : En cas de sinistre ou d'incident majeur sur le site du serveur, si celui-ci a perdu son certificat, il en génère un nouveau automatiquement lors de sa récupération. Il faut alors importer ce nouveau certificat sur chaque client.

5. Une fois le certificat du serveur ajouté à la base de données dsmcert.kdb du client, ajoutez l'option `ssl yes` au fichier `C:\Windows\SysWOW64\fb.opt` et mettez à jour la valeur de l'option `tcpport`.

   Important :

   Le serveur est généralement configuré pour recevoir les connexions SSL ou TLS sur un port différent de celui des connexions non SSL ou non TLS. Ne spécifiez pas de numéro de port non SSL ou non TLS pour la valeur de `tcpport`. Si la valeur de `tcpport` est incorrecte, l'agent de récupération ne pourra pas se connecter au serveur.

   Il n'est pas possible de connecter à un port non SSL ou non TLS un agent de récupération configuré pour communiquer en mode SSL ou TLS. Inversement, il n'est pas possible de connecter à un port SSL ou TLS un agent de récupération qui n'est pas configuré pour communiquer en mode SSL ou TLS.

6. Spécifiez les ports SSL ou TLS corrects dans les fichiers de configuration suivants de l'agent de récupération :
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

Activation de la communication sécurisée en utilisant un certificat tiers

Si le serveur IBM Spectrum Protect utilise un certificat tiers, vous devez obtenir le certificat racine de l'autorité de certification (CA).

Pourquoi et quand exécuter cette tâche

Si le certificat a été émis par une autorité de certification telle que Symantec ou Thawte, le client est d'ores et déjà prêt à utiliser SSL ou TLS et vous pouvez omettre les étapes de configuration qui suivent. Pour obtenir la liste des certificats racines de CA préinstallés, recherchez **Certificats racine des autorités de certification** dans l'IBM Knowledge Center.

Si le certificat n'a pas été émis par le biais d'un certificat racine de CA préinstallé, ou s'il s'agit d'un certificat de CA "maison", géré en interne par votre société, vous devez configurer Recovery Agent de sorte qu'il communique avec le serveur en utilisant le protocole SSL ou TLS.

Procédure

Pour permettre à l'agent de récupération de communiquer avec le serveur par SSL ou TLS avec un certificat de CA :

1. Ajoutez à la variable d'environnement PATH du client le chemin des binaires du GSKit ainsi que celui des bibliothèques. Par exemple :

   ```
   set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
       C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. S'il s'agit de la première configuration de SSL ou TLS sur le client, vous devez créer sa base de données de clés locale, dsmcert.kdb. A partir du répertoire `C:\Windows\SysWOW64` du client, lancez la commande **gsk8capicmd_64** comme dans l'exemple suivant :

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw mot_de_passe -stash
   ```

   Le mot de passe que vous fournissez sert à chiffrer la base de données de clés. Le mot de passe est automatiquement stocké sous forme chiffrée dans le fichier de dissimulation (dsmcert.sth). Ce fichier est utilisé par le client pour obtenir le mot de passe de la base de données de clés.
3. Obtenez le certificat de l'autorité de certification.
4. Importez le certificat dans la base de données dsmcert.kdb. Le certificat doit être importé dans la base de données de clés de chaque client. A partir du répertoire `C:\Windows\SysWOW64` du client, lancez la commande **gsk8capicmd_64** comme dans l'exemple suivant :

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Autorité de certification XYZ"
   -file chemin_certificat_racine_CA -format ascii -trust enable
   ```

   Plusieurs certificats de différents serveurs peuvent être ajoutés à la base de données dsmcert.kdb afin que le client puisse se connecter à ces serveurs. Chaque certificat doit avoir son propre label. Utilisez un nom significatif pour chacun.

   Important : En cas de sinistre ou d'incident majeur sur le site du serveur, si celui-ci a perdu son certificat, il en génère un nouveau automatiquement lors de sa récupération. Il faut alors importer ce nouveau certificat sur chaque client.
5. Une fois le certificat du serveur ajouté à la base de données dsmcert.kdb du client, ajoutez l'option `ssl yes` au fichier `C:\Windows\SysWOW64\fb.opt` et mettez à jour la valeur de l'option `tcpport`.

   Important :

   Le serveur est généralement configuré pour recevoir les connexions SSL ou TLS sur un port différent de celui des connexions non SSL ou non TLS. Ne spécifiez pas de numéro de port non SSL ou non TLS pour la valeur de `tcpport`. Si la valeur de `tcpport` est incorrecte, l'agent de récupération ne pourra pas se connecter au serveur.

   Il n'est pas possible de connecter à un port non SSL ou non TLS un agent de récupération configuré pour communiquer en mode SSL ou TLS. Inversement, il n'est pas possible de connecter à un port SSL ou TLS un agent de récupération qui n'est pas configuré pour communiquer en mode SSL ou TLS.
6. Spécifiez les ports SSL ou TLS corrects dans les fichiers de configuration suivants de l'agent de récupération :
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

Paramètres régionaux

Les paramètres régionaux identifient la langue utilisée pour les interfaces, les messages et l'aide en ligne.

Interfaces graphiques de Data Protection for VMware

Le terme «Interface graphique de Data Protection for VMware» se réfère aux interfaces graphiques suivantes :

- Interface graphique de Data Protection for VMware vSphere accessible dans un navigateur Web
- Le Plug-in client IBM Spectrum Protect vSphere dans l'interface graphique client Web vSphere

Les interfaces graphiques de Data Protection for VMware ne peuvent pas s'exécuter dans un environnement avec des paramètres régionaux incohérents sur les processeurs exécutant l'interface graphique de Data Protection for VMware, le client VMware vSphere, et le serveur IBM Spectrum Protect.

Spécifiez les mêmes paramètres régionaux sur tous les systèmes exécutant l'interface graphique de Data Protection for VMware, le client VMware vSphere et le serveur IBM Spectrum Protect.

Lors du tout premier accès à une page d'aide de l'interface graphique de Data Protection for VMware via le lien "En savoir plus", l'aide s'affiche dans la langue spécifiée dans les paramètres régionaux du système sur lequel s'exécute l'interface graphique de Data Protection for VMware. Lors du premier accès à l'aide, celle-ci ne s'affiche pas dans la langue spécifiée dans les paramètres régionaux du client VMware vSphere. Dans ce cas, une fois la page d'aide de l'interface graphique Data Protection for VMware affichée, cliquez sur deux liens au moins, puis fermez la page d'aide. La prochaine fois que l'aide est lancée via le lien "En savoir plus", elle s'affiche dans la langue spécifiée dans les paramètres régionaux du client VMware vSphere.

Interface de restauration de fichier de IBM Spectrum Protect

Le contenu de l'interface et la langue de l'invite de message sont déterminés par le paramètre de langue du navigateur Web accédant à l'interface de restauration de fichier de IBM Spectrum Protect.

Pour les messages d'erreur consignés dans le fichier `fr_api.log`, l'interface de restauration de fichier de IBM Spectrum Protect utilise la langue spécifiée par le paramètre de langue du système sur lequel s'exécute l'Interface graphique de Data Protection for VMware vSphere.

Activité de consignation au journal

Data Protection for VMware crée et modifie plusieurs journaux lors des opérations d'installation, de sauvegarde, de montage et de restauration.

Les journaux de Data Protection for VMware sont des fichiers en texte clair qui utilisent une extension de fichier `.sf`.

Windows Les journaux sont implantés dans le répertoire suivant :
`%ALLUSERSPROFILE%\Tivoli\TSM\TDPVMware`

Les répertoires comportent un sous-répertoire pour chaque composant Data Protection for VMware. Par exemple, pour Recovery Agent il s'agit du sous-répertoire `\mount` et pour l'interface de ligne de commande de l'agent de récupération, du sous-répertoire `\shell`.
Vous pouvez rechercher des fichiers journaux depuis le menu **Windows** > **Démarrer** en sélectionnant **Panneau de configuration** > **Rechercher** et en entrant `*.log`.

Linux Les journaux sont implantés sous les deux chemins suivants :
`<rép.utilisateur>/tivoli/tsm/ve/mount/log`
`/opt/tivoli/tsm/TDPVMware/mount/engine/var`
Vous pouvez rechercher des fichiers journaux en entrant la commande suivante :

```
find /opt/tivoli/ -name "*.log"
```

Important : Les fichiers journaux existants sont écrasés chaque fois qu'une installation est lancée. Si un problème survient lors de l'installation et qu'il vous faut réinstaller le produit, récupérez le fichier `TDPVMwareInstallation.log` existant depuis le répertoire `%allusersprofile%` avant de relancer l'installation.

Remarque : Lorsque le service Data Protection for VMware est en opération, plusieurs journaux sont conservés à l'état ouvert. Par conséquent, certains gestionnaires de fichier n'affichent pas l'état actuel de ces fichiers et peuvent indiquer une taille de fichier égale à zéro. La sélection ou l'ouverture d'un de ces fichiers force le gestionnaire de fichiers à mettre à jour les informations sur ce fichier.

Fichiers journaux Recovery Agent

Le fichier journal de Recovery Agent se nomme `TDP_FOR_VMWARE_MOUNT`*`nnn`*`.sf`. Le fichier journal contenant les données les plus récentes est stocké dans le fichier journal portant le numéro *040* (`TDP_FOR_VMWARE_MOUNT040.sf`). Lorsqu'un fichier journal atteint la taille maximale autorisée, un nouveau journal est créé. Le nom du fichier journal est identique si ce n'est que son numéro diminue d'une unité. Spécifiquement, les données du fichier journal portant le numéro *040* sont copiées dans un fichier journal portant le numéro *039*. Le fichier journal portant le numéro *040* contient les données les plus récentes. Lorsque *040* atteint à nouveau la taille de fichier maximale, le contenu du fichier *039* passe au fichier *038* et les informations du fichier *040* passent à nouveau au fichier *039*.

Fichiers journaux de l'interface graphique de Data Protection for VMware

Interface graphique de Data Protection for VMware vSphere place les fichiers journaux dans le répertoire suivant :

Windows `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs`

Lorsque vous collectez les fichiers journaux, prenez soin d'inclure tous les sous-répertoires dans votre fichier compressé.

Fichiers journaux Interface de ligne de commande Data Protection for VMware

L'Interface de ligne de commande Data Protection for VMware place les fichiers journaux dans le répertoire suivant :

Windows C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\logs

Linux /opt/tivoli/tsm/tdpvmware/common/logs

Lorsque vous collectez les fichiers journaux, prenez soin d'inclure tous les sous-répertoires dans votre fichier compressé.

Fichiers journaux de l'interface de restauration de fichier de IBM Spectrum Protect

L'interface de restauration de fichier de IBM Spectrum Protect consigne les messages d'erreur dans les fichiers `fr_api.log`, `fr_gui.log` et `messages.log`. Ces fichiers résident dans le répertoire par défaut suivant :

Windows C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs

Linux /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs

Vous pouvez modifier le nom et l'emplacement du fichier `fr_api.log` en configurant les options `API_LOG_FILE_NAME` et `API_LOG_FILE_LOCATION` dans le journal d'activité de restauration de fichiers (`FRLog.config`).

Les opérations de restauration de fichier sont également consignées par le serveur IBM Spectrum Protect. Vous pouvez rechercher ces messages à l'aide d'un client de ligne de commande d'administration du serveur.

- Pour lancer une session de client d'administration en mode de ligne de commande, entrez la commande suivante sur votre poste de travail :

  ```
  dsmadmc -id=admin -password=admin -dataonly=yes
  ```

  En entrant la commande **DSMADMC** avec les options **-ID** et **-PASSWORD** comme illustré, vous n'êtes pas invité à entrer un ID et un mot de passe utilisateur.
- Pour effectuer une recherche dans le tableau étendu de récapitulatif SQL afin d'examiner les résultats des opérations de restauration de fichiers, lancez la commande **select** depuis le client de ligne de commande d'administration :

  ```
  select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
  ```

  Vous pouvez circonscrire la recherche en utilisant un ou plusieurs des critères suivants dans l'instruction select :

  - * ENTITY='*NOM_NOEUD_DISPOSIF_TRANSFERT_DONNEES*'
  - * AS_ENTITY='*NOM_NOEUD_CENTRE_DONNEES*'
  - * SUB_ENTITY='*NOM_HOTE_MACHINE_VIRTUELLE*'
  - * START_TIME='*aaaa-MM-jj HH:mm:ss*'

  Par exemple :

  ```
  select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
  and ENTITY='LOCAL_MP_WIN' and AS_ENTITY='DC_NODE' and SUB_ENTITY='testvm'
  and START_TIME>'2017-03-11 17:30:00'
  ```

  Le critère `START_TIME` gère des requêtes avec les signes suivants : égal (=), inférieur à (<), ou supérieur à (>).
- Pour effectuer une recherche dans le tableau de journal d'activité SQL pour examiner les événements des opérations de restauration de fichiers, lancez la commande **select** depuis le client de ligne de commande d'administration :

  ```
  select * from ACTLOG
  ```

  Vous pouvez circonscrire la recherche en utilisant un ou plusieurs des critères suivants dans l'instruction select :

– * NODENAME='*NOM_NOEUD_CENTRE_DONNEES*'
– * DATE_TIME='*aaa-MM-jj HH:mm:ss*'

Par exemple :

```
select * from ACTLOG where NODENAME='DC_NODE' and DATE_TIME>'2017-03-11 17:30:00'
```

Spécifiez les éléments *NOM_NOEUD_DISPOSIF_TRANSFERT_DONNEES* et *NOM_NOEUD_CENTRE_DONNEES* en majuscules.

Le critère DATE_TIME gère des requêtes avec les signes suivants : égal (=), inférieur à (<), ou supérieur à (>).

Démarrage et exécution de services pour Data Protection for VMware

Par défaut, lorsque vous démarrez le système d'exploitation Windows, Recovery Agent démarre sous le compte système local.

Exécution des services Recovery Agent sous Microsoft Windows

Lorsque vous démarrez Recovery Agent à partir du menu Démarrer de Windows, le service est automatiquement arrêté. Si Recovery Agent, lancé à partir du menu Démarrer, prend fin, le service démarre automatiquement. De plus, pour ces systèmes d'exploitation, le service ne propose pas d'interface graphique. Pour utiliser l'interface graphique, accédez au menu Windows Démarrer et sélectionnez **Tous les programmes** > **IBM Spectrum Protect** > **Data Protection for VMware** > **Recovery Agent**.

Interface de ligne de commande Data Protection for VMware

Vous pouvez vérifier que l'Interface de ligne de commande Data Protection for VMware est en cours d'exécution comme suit :

Windows Cliquez sur **Démarrer** > **Panneau de configuration** > **Outils d'administration** > **Services** et vérifiez que l'état de Interface de ligne de commande Data Protection for VMware est Démarré.

Linux Accédez au répertoire des scripts (/opt/tivoli/tsm/tdpvmware/common/scripts/) et exécutez la commande suivante :

```
./vmclid status
```

- Si le démon n'est pas en cours d'exécution, exécutez la commande suivante pour le démarrer manuellement :

  ```
  /opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
  ```

  Ces scripts init peuvent également être utilisés pour arrêter et démarrer le démon :

  ```
  ./vmclid stop
  ./vmclid start
  ```

Annexe A. Tâches de configuration avancées

Vous devez configurer manuellement et vérifier chaque composant à l'aide des interfaces d'application disponibles.

Avant de commencer

Avant de poursuivre l'exécution de cette tâche, vérifiez que les conditions suivantes existent :

- Un serveur IBM Spectrum Protect doit être disponible pour enregistrer les noeuds.
- L'Interface graphique de Data Protection for VMware vSphere est installée sur un système respectant les exigences en matière de système d'exploitation. Elle doit disposer d'une connexion réseau avec les systèmes suivants :
  - Serveur de sauvegarde vStorage
  - Serveur IBM Spectrum Protect
  - Serveur vCenter

Procédure

1. Connectez-vous au serveur IBM Spectrum Protect et exécutez les tâches décrites à la section «Configuration des noeuds IBM Spectrum Protect dans un environnement vSphere», à la page 94.
2. Connectez-vous au serveur de sauvegarde vStorage et exécutez les tâches décrites à la section «Configuration de noeuds de dispositif de transfert de données avec l'interface graphique du plug-in vSphere», à la page 95.
3. Connectez-vous au système sur lequel l'Interface graphique de Data Protection for VMware vSphere est installée et exécutez les tâches décrites à la section «Configuration de l'Interface de ligne de commande Data Protection for VMware dans un environnement vSphere», à la page 102.
4. Sur le système où l'Interface graphique de Data Protection for VMware vSphere est installée, démarrez le client vSphere et connectez-vous à vCenter. Si le client vSphere est déjà en cours d'exécution, vous devez l'arrêter et le redémarrer.
5. Accédez au répertoire de base dans le client vSphere. Cliquez sur l'icône de l'Interface graphique de Data Protection for VMware vSphere dans le panneau Solutions et applications.

   Conseil : Si l'icône n'apparaît pas, l'Interface graphique de Data Protection for VMware vSphere n'a pas été enregistrée ou une erreur de connexion s'est produite.

   a. Dans le menu du client vSphere, accédez à **Plug-ins** > **Manage Plug-ins** pour démarrer le gestionnaire de plug-in.
   b. Si vous pouvez localiser l'Interface graphique de Data Protection for VMware vSphere et qu'une erreur de connexion s'est produite, vérifiez la connectivité à la machine sur laquelle l'Interface graphique de Data Protection for VMware vSphere est installée en exécutant la commande `ping`.

Résultats

L'Interface graphique de Data Protection for VMware vSphere est prête pour les opérations de sauvegarde et restauration.

Configuration des noeuds IBM Spectrum Protect dans un environnement vSphere

Cette procédure décrit la marche à suivre pour enregistrer manuellement les noeuds auprès du serveur IBM Spectrum Protect et leur accorder des droits de proxy dans un environnement vSphere.

Avant de commencer

Important :

Pourquoi et quand exécuter cette tâche

Toutes les étapes de cette procédure sont effectuées sur le serveur IBM Spectrum Protect.

Conseil : Cette tâche peut également être effectuée à l'aide de l'assistant de configuration ou du bloc-notes d'édition de la configuration de l'Interface graphique de Data Protection for VMware vSphere. Lancez l'Interface graphique de Data Protection for VMware vSphere en ouvrant un navigateur Web et en accédant au serveur Web de l'interface. Par exemple :

```
https://guihost.mycompany.com:9081/TsmVMwareUI/
```

Connectez-vous à l'aide du nom d'utilisateur et du mot de passe vCenter.

- Pour une configuration initiale, accédez à **Configuration** > **Lancer l'assistant de configuration**.
- Pour une configuration existante, accédez à **Configuration** > **Modifier la configuration**.

Procédure

1. Connectez-vous au serveur IBM Spectrum Protect et démarrez une session client d'administration en mode de ligne de commande :

   ```
   dsmadmc -id=admin -password=admin -dataonly=yes
   ```

2. Exécutez la commande `REGister Node` pour enregistrer les noeuds suivants auprès du noeud IBM Spectrum Protect :

   a. Le noeud qui représente le serveur VMware vCenter (noeud vCenter) :

      ```
      REGister Node MY_VCNODE <mot de passe de MY_VCNODE>
      ```

   b. Le noeud qui communique entre IBM Spectrum Protect et l'Interface graphique de Data Protection for VMware vSphere (noeud VMCLI) :

      ```
      REGister Node MY_VMCLINODE <mot de passe de MY_VMCLINODE>
      ```

   c. Le noeud qui représente le centre de données et dans lequel les données de la machine virtuelle sont stockées (noeud du centre de données) :

      ```
      REGister Node MY_DCNODE <mot de passe de MY_DCNODE>
      ```

   d. Le noeud qui "déplace les données" d'un système à un autre (noeud de dispositif de transfert de données) :

      ```
      REGister Node MY_DMNODE <mot de passe de MY_DMNODE>
      ```

Avertissement : Lors de l'enregistrement des noeuds auprès du serveur IBM Spectrum Protect, n'utilisez pas le paramètre `userid`.

3. Exécutez la commande `GRant PROXynode` pour définir des relations de proxy pour ces noeuds :

   A faire : Les noeuds cible sont les propriétaires des données et les noeuds d'agent agissent au nom des noeuds cible. Lorsqu'il bénéficie des droits de proxy pour accéder à un noeud, un noeud d'agent peut exécuter des opérations de sauvegarde et de restauration pour le noeud cible.

   a. Accordez un droit de proxy au noeud vCenter en exécutant la commande suivante :

      ```
      GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
      ```

      Cette commande accorde à `MY_DCNODE` et à `MY_VMCLINODE` les droits nécessaires pour sauvegarder et restaurer des machines virtuelles pour le compte de `MY_VCNODE`.

   b. Accordez un droit de proxy au noeud du centre de données en exécutant la commande suivante :

      ```
      GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
      ```

      Cette commande accorde à `MY_VMCLINODE` et à `MY_DMNODE` les droits nécessaires pour sauvegarder et restaurer des machines virtuelles pour le compte de `MY_DCNODE`.

   c. (Facultatif) Accordez les droits en tant que proxy à tout autre noeud du centre de données ou noeud de dispositif de transfert de données de votre environnement.

   d. Vérifiez les relations de proxy en exécutant la commande `Query PROXynode` du serveur IBM Spectrum Protect. Le résultat attendu est le suivant : Le résultat attendu de la commande est :

      ```
      Noeud cible       Noeud d'agent
      --------------    ------------------------------
      MY_VCNODE           MY_DCNODE  MY_VMCLINODE
      MY_DCNODE           MY_VMCLINODE  MY_DMNODE
      ```

Que faire ensuite

Une fois les noeuds IBM Spectrum Protect configurés, la tâche de configuration suivante consiste à configurer les noeuds de dispositif de transfert de données conformément à la description donnée dans «Configuration de noeuds de dispositif de transfert de données avec l'interface graphique du plug-in vSphere».

Configuration de noeuds de dispositif de transfert de données avec l'interface graphique du plug-in vSphere

Si vous déchargez des charges de travail de sauvegarde sur un serveur de sauvegarde vStorage dans un environnement vSphere, vous pouvez utiliser l'assistant du dispositif de transfert de données pour configurer une série de noeuds de dispositif de transfert de données afin qu'ils exécutent cette opération et déplacent les données vers le serveur IBM Spectrum Protect.

Avant de commencer

La configuration de noeuds de dispositif de transfert de données implique des changements de configuration, le démarrage des services nécessaires et la vérification de la configuration.

Vous pouvez effectuer ces tâches à l'aide de l'interface graphique du plug-in qui simplifie et accélère la création d'une série de noeuds de dispositif de transfert de données. Vous pouvez également procéder manuellement ; pour plus d'informations, voir «Configuration manuelle des noeuds de dispositif de transfert de données dans un environnement vSphere», à la page 97.

Dans un environnement Data Protection for VMware standard, un fichier `dsm.opt` distinct (Windows) ou une section du fichier `dsm.sys` (Linux) est utilisé pour chaque noeud de dispositif de transfert de données. Lorsque plusieurs noeuds de dispositif de transfert de données d'un serveur de sauvegarde vStorage sont utilisés pour le dédoublonnage de données et disposent des droits d'accès nécessaires pour transférer des données concernant le même noeud du centre de données, chaque fichier `dsm.opt` ou section du fichier `dsm.sys` doit inclure une valeur différente de l'option `dedupcachepath`.

Un noeud de dispositif de transfert de données physique utilise généralement les réseaux de stockage SAN pour sauvegarder et restaurer les données. Si vous configurez le noeud du dispositif de transfert de données pour accéder directement aux volumes de stockage, désactivez l'affectation automatique de l'identificateur d'unité. Si vous ne désactivez pas l'affectation des lettres d'unités, le client présent sur le noeud de dispositif de transfert de données peut endommager le mappage de données brutes des disques virtuels. Si ce mappage est endommagé, les sauvegardes échouent.

Restriction : Data Protection for VMware ne prend pas en charge la planification du serveur de sauvegarde vStorage (utilisé en tant que dispositif de transfert de données) pour se sauvegarder. Assurez-vous que le serveur de sauvegarde vStorage est exclu de ses propres planifications. Utilisez un autre serveur de sauvegarde vStorage pour effectuer la sauvegarde d'une machine virtuelle vStorage contenant un serveur de sauvegarde.

Si vous devez effectuer l'un des ajustements indiqués ci-dessus, consultez la rubrique "Configuration manuelle des noeuds de dispositif de transfert de données dans un environnement vSphere".

Pourquoi et quand exécuter cette tâche

Utilisez le plug-in vSphere pour configurer les noeuds de dispositif de transfert de données.

Procédure

1. A partir du plug-in vSphere, sélectionnez IBM Spectrum Protect.
2. Sur l'onglet **Configurer**, sélectionnez **Dispositifs de transfert de données**.
3. Dans le panneau **Ajouter un dispositif de transfert de données**, sélectionnez un centre de données dans le menu déroulant.
4. Editez, si nécessaire, les zones suivantes :

- **Nom du dispositif de transfert de données** : nom de noeud, déjà renseigné avec une suggestion de nom basée sur le préfixe du noeud, le nom de noeud du centre de données, le nom du dispositif de transfert de données et un numéro d'incrémentation.
- **Nom d'hôte du dispositif de transfert de données**
- **Utilisateur vCenter**, déjà renseigné avec le nom de l'utilisateur ayant enregistré le plug-in.
- **Mot de passe vCenter**

Cliquez sur **Ajouter** une fois les paramètres indiqués.

5. L'écran **Résultats** affiche :
   - le nom du dispositif de transfert de données configuré,
   - l'emplacement du fichier d'options ; vous pouvez configurer le dispositif de transfert de données en éditant ce fichier,
   - l'emplacement des fichiers journaux,
   - les options par défaut qui ont été utilisées.
6. Vous pouvez maintenant tester le dispositif de transfert de données via l'onglet de configuration des dispositifs de transfert de données d'IBM Spectrum Protect. Vous pouvez également vérifier l'installation en sélectionnant le dispositif de transfert de données et en cliquant sur **Vérifier**, ou en vérifiant le statut lors de la prochaine installation d'un dispositif de transfert de données.
7. Vous pouvez ajouter le dispositif de transfert de données à une planification via l'onglet des planifications d'IBM Spectrum Protect.

Configuration manuelle des noeuds de dispositif de transfert de données dans un environnement vSphere

Si vous déchargez des charges de travail de sauvegarde sur un serveur de sauvegarde vStorage dans un environnement vSphere, vous pouvez configurer manuellement les noeuds de dispositif de transfert de données afin qu'ils exécutent cette opération et déplacent les données vers le serveur IBM Spectrum Protect.

Avant de commencer

Un noeud de dispositif de transfert de données physique utilise généralement les réseaux de stockage SAN pour sauvegarder et restaurer les données. Si vous configurez les noeuds de dispositif de transfert de données afin qu'il accèdent directement aux volumes de stockage, désactivez l'affectation automatique de l'identificateur d'unité. Si vous ne désactivez pas l'affectation des lettres d'unités, le client présent sur le noeud de dispositif de transfert de données peut endommager le mappage de données brutes des disques virtuels. Si ce mappage est endommagé, les sauvegardes échouent.

Services requis : Le dispositif de transfert de données requiert le service d'accepteur client, le service d'agent d'accepteur client et le service du planificateur de dispositifs de transfert de données, comme indiqué dans les étapes ci-dessous. Si vous retirez un dispositif de transfert de données dans un centre de données, désinstallez et supprimez ces services pour le dispositif de transfert de données.

Important : Si le dispositif de transfert de données est installé sur le même système Windows que l'interface graphique Data Protection for VMware vSphere et que l'option **Créer des services** a été sélectionnée lors de la configuration du dispositif de transfert de données, vous devez suivre les étapes ci-après.

Dans un environnement Data Protection for VMware standard, un fichier `dsm.opt` distinct (Windows) ou une section du fichier `dsm.sys` (Linux) est utilisé pour chaque noeud de dispositif de transfert de données. Lorsque plusieurs noeuds de dispositif de transfert de données d'un serveur de sauvegarde vStorage sont utilisés pour le dédoublonnage de données et disposent des droits d'accès nécessaires pour transférer des données concernant le même noeud du centre de données, chaque fichier `dsm.opt` ou section du fichier `dsm.sys` doit inclure une valeur différente de l'option `dedupcachepath`. Pour optimiser les résultats, définissez des options `schedlogname` et `errorlogname` différentes pour chaque fichier `dsm.opt` ou section du fichier `dsm.sys`. L'ensemble d'options minimum requis est décrit à l'étape 2.

Un noeud de dispositif de transfert de données physique utilise généralement les réseaux de stockage SAN pour sauvegarder et restaurer les données. Si vous configurez le noeud du dispositif de transfert de données pour accéder directement aux volumes de stockage, désactivez l'affectation automatique de l'identificateur d'unité. Si vous ne désactivez pas l'affectation des lettres d'unités, le client présent sur le noeud de dispositif de transfert de données peut endommager le mappage de données brutes des disques virtuels. Si ce mappage est endommagé, les sauvegardes échouent.

Restriction : Data Protection for VMware ne prend pas en charge la planification du serveur de sauvegarde vStorage (utilisé en tant que dispositif de transfert de données) pour se sauvegarder. Assurez-vous que le serveur de sauvegarde vStorage est exclu de ses propres planifications. Utilisez un autre serveur de sauvegarde vStorage pour effectuer la sauvegarde d'une machine virtuelle vStorage contenant un serveur de sauvegarde.

Pourquoi et quand exécuter cette tâche

Conseil : Toutes les étapes de cette procédure sont effectuées sur le serveur de sauvegarde vStorage.

Procédure

1. Linux Vérifiez que le logiciel Java est installé sur la machine cible.
2. Linux Définissez les variables d'environnement appropriées.
   a. Vérifiez que la variable d'environnement `JAVA_HOME` est correctement exportée :
      ```
      export JAVA_HOME=<jre-or-jdk-install-dir>
      ```
   b. Vérifiez que la variable d'environnement `PATH` est correctement exportée :
      ```
      export PATH=$PATH:$JAVA_HOME/jre/bin
      ```
   c. Vérifiez que la variable d'environnement `LD_LIBRARY_PATH` est correctement exportée. Vérifiez les paramètres ou définissez-la sur le répertoire d'installation du client et la bibliothèque partagée Java `libjvm.so` :

      Pour IBM Java :
      ```
      export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/bin/classic
      ```
      Pour Oracle Java :
      ```
      export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/lib/amd64/server
      ```
3. Créez le fichier d'options `dsm.opt` ou `dsm.sys` à l'emplacement suivant :
   - **Windows :** `C:\Program Files\Tivoli\TSM\baclient`
   - **Linux :** `/opt/tivoli/tsm/client/ba/bin`

4. Copiez les options de l'exemple de fichier d'options du dispositif de transfert de données dans le fichier `dsm.opt` ou `dsm.sys`. Pour trouver l'exemple de fichier du dispositif de transfert de données, procédez comme suit :
   - Ouvrez un navigateur Web et entrez l'adresse du serveur Web de l'interface graphique. Par exemple :
     `https://guihost.mycompany.com:9081/TsmVMwareUI/`
   - Connectez-vous à l'aide du nom d'utilisateur et du mot de passe vCenter et vérifiez que l'option **Mode de configuration** est sélectionnée.
   - Dans l'assistant de configuration, accédez à la page Noeuds de dispositif de transfert de données.
   - Recherchez le dispositif de transfert de données de votre choix et cliquez sur **Visualiser**.
   - Copiez l'exemple d'options de l'onglet **Windows** ou **Linux** dans le fichier d'options.

   Vous pouvez mettre à jour ces options pour votre environnement, si nécessaire.

   Pour obtenir une description des options, reportez-vous aux informations de référence sur les options.

   Pour les opérations d'accès instantané, de restauration instantanée ou de montage (restauration de fichiers), veillez à ajouter `VMISCSISERVERADDRESS` au fichier d'options du dispositif de transfert de données. Spécifiez l'adresse IP de serveur iSCSI de la carte réseau sur le serveur de sauvegarde vStorage utilisé pour le transfert des données iSCSI au cours des opérations instantanées. La carte d'interface réseau physique (NIC) qui est liée au périphérique iSCSI se trouvant sur l'hôte ESX doit se trouver sur le même sous-réseau que la carte présente sur le serveur de sauvegarde vStorage utilisé pour le transfert iSCSI.
5. Lancez la commande suivante pour définir le nom d'utilisateur et le mot de passe VMware vCenter associés au noeud de dispositif de transfert de données :
   ```
   dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
   ```
6. Configurez le service d'accepteur client et le service du planificateur de transfert de données en exécutant les tâches suivantes :
   - Windows Cette procédure utilise l'assistant de configuration de l'interface graphique du client IBM Spectrum Protect pour configurer le service d'accepteur client et le service du planificateur. Par défaut, le service d'agent du client distant est également configuré à l'aide de l'assistant. Si vous vous servez de l'utilitaire de configuration du service client IBM Spectrum Protect (**`dsmcutil`**) pour cette tâche, assurez-vous d'installer également le service d'agent du client distant.

     Lancez l'assistant de configuration du client IBM Spectrum Protect en sélectionnant **Utilitaires** > **Assistant de configuration** dans le menu Fichier :
     - Sélectionnez **Aide à la configuration du client Web TSM**. Entrez les informations demandées par le système.
       a. Dans l'option `Quand souhaitez-vous démarrer le service ?`, sélectionnez **Automatiquement au démarrage de Windows**.
       b. Dans l'option `Voulez-vous démarrer le service dès la fin de cet assistant ?`, sélectionnez **Oui**.

       Une fois l'opération terminée, revenez à la page d'accueil de l'assistant et passez à l'étape b.

Conseil : Lorsque vous configurez plusieurs noeuds de dispositif de transfert de données sur la même machine, vous devez indiquer une valeur de port pour chaque instance d'accepteur client.

– Sélectionnez `Aide à la configuration du planificateur de client TSM`. Entrez les informations demandées par le système.

a. Lorsque vous saisissez le nom du planificateur, veillez à sélectionner l'option **Utiliser le démon Client Acceptor (CAD) pour gérer le planificateur**.

b. Dans l'option `Quand souhaitez-vous démarrer le service ?`, sélectionnez **Automatiquement au démarrage de Windows**.

c. Dans l'option `Voulez-vous démarrer le service dès la fin de cet assistant ?`, sélectionnez **Oui**.

- Linux **Pour le dispositif de transfert de données sous Linux, procédez comme suit :**

a. le programme d'installation crée un script de démarrage pour l'accepteur client (`dsmcad`) dans `/etc/init.d`. Vérifiez ou définissez les variables d'environnement appropriées dans `/etc/init.d/dsmcad file`.

b. Spécifiez les options suivantes dans le fichier `dsm.sys`, dans la section du noeud de dispositif de transfert de données :

– Spécifiez l'option `managedservices` avec ces deux paramètres :

```
managedservices schedule webclient
```

Ce paramètre ordonne à l'accepteur client de gérer à la fois le client Web et le planificateur.

– (Facultatif) Si vous souhaitez acheminer des informations de planification et d'erreur vers des fichiers journaux autres que les fichiers par défaut, spécifiez les options `schedlogname` et `errorlogname` avec le chemin et le nom de fichier complet dans lequel vous souhaitez stocker les informations de journal. Par exemple :

```
schedlogname /vmsched/dsmsched_dm.log
errorlogname /vmsched/dsmerror_dm.log
```

c. Démarrez le service d'accepteur client :

Pour pouvoir gérer les tâches du planificateur ou le client Web, l'accepteur client doit avoir démarré. En tant que superutilisateur, exécutez les tâches suivantes :

1) Configurez le service d'accepteur client et le service du planificateur de transfert de données pour qu'ils fassent office de serveur de sauvegarde vStorage.

2) Exécutez la commande suivante pour démarrer l'accepteur client :

```
service dsmcad start
```

Pour activer le démarrage automatique de l'accepteur client après un redémarrage du système, à l'invite shell, ajoutez le service en procédant comme suit :

```
# chkconfig --add dsmcad
```

Conseil : Si vous voulez exécuter la commande **dsmc** directement à partir de la ligne de commande Linux, vous devez également appliquer les variables d'environnement équivalentes mentionnées à l'étape 2 à l'interpréteur de commandes.

7. Lancez une session de ligne de commande du dispositif de transfert de données avec les paramètres `-asnodename` et `-optfile` :

```
dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt
```

Vérifiez qu'après votre connexion initiale, vous n'êtes pas invité à entrer votre mot de passe.

Avertissement : Pour éviter tout échec du planificateur IBM Spectrum Protect, vérifiez que l'option `asnodename` n'est pas définie dans le fichier `dsm.opt` (Windows) ou la section du fichier `dsm.sys` (Linux). Le planificateur demande au serveur IBM Spectrum Protect les planifications associées au `nodename` (nom du dispositif de transfert de données) et non au `asnodename` (noeud du centre de données). Si `asnodename` est défini dans `dsm.opt` ou `dsm.sys`, les planifications associées à `asnodename` (et non à `nodename`) sont demandées. Par conséquent, les opérations de planification échouent.

Effectuez les tâches suivantes :

a. Vérifiez la connexion au serveur IBM Spectrum Protect en exécutant la commande suivante :

   ```
   dsmc query session
   ```

   Cette commande affiche des informations sur votre session, notamment le nom de noeud en cours, la date et l'heure d'établissement de session, ainsi que des informations sur le serveur et sur la connexion serveur.

b. Vérifiez que vous pouvez sauvegarder une machine virtuelle en exécutant la commande suivante :

   ```
   dsmc backup vm vm1
   ```

   A l'étape 5b et 5d, `vm1` est le nom de la machine virtuelle.

c. Vérifiez que la sauvegarde s'est correctement effectuée en exécutant cette commande :

   ```
   dsmc query vm "*"
   ```

d. Vérifiez que la machine virtuelle peut être restaurée en exécutant la commande suivante :

   ```
   dsmc restore vm vm1 -vmname=vm1-restore
   ```

8. Vérifiez que l'accepteur client et l'agent sont configurés correctement :

   a. Dans un navigateur Web, entrez l'adresse du plug-in client IBM Spectrum Protect vSphere. Par exemple :

      ```
      https://guihost.mycompany.com/vsphere-client/
      ```

   b. Connectez-vous avec le nom d'utilisateur et le mot de passe vCenter.

   c. Dans vSphere Web Client, cliquez sur **IBM Spectrum Protect** > **Configurer** > **Dispositifs de transfert de données**.

   d. Vérifiez que la mention **Vérifié** apparaît dans la colonne **Statut** du dispositif de transfert de données. Si la mention **Echec** apparaît, placez le pointeur de la souris sur le statut pour afficher le message d'échec.

   Conseil : Lorsque l'adresse IP change sur le système sur lequel l'Interface graphique de Data Protection for VMware vSphere est installée, vous devez procéder ainsi :

   a. Reconfigurez l'accepteur client afin que l'Interface graphique de Data Protection for VMware vSphere soit activée pour les opérations. Faute de quoi, le gestionnaire de plug-in affiche l'état de l'Interface graphique de Data Protection for VMware vSphere comme désactivée.

Configuration de l'Interface de ligne de commande Data Protection for VMware dans un environnement vSphere

Mettez à jour le profil de l'Interface de ligne de commande Data Protection for VMware sur le système sur lequel l'Interface graphique de Data Protection for VMware vSphere est installée.

Avant de commencer

Le profil (`vmcliprofile`) se trouve dans le répertoire suivant sur le système sur lequel l'Interface graphique de Data Protection for VMware vSphere est installée :

Linux `/opt/tivoli/tsm/tdpvmware/common/scripts`

Windows 64 bits : `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts`

Pourquoi et quand exécuter cette tâche

Toutes les étapes de cette procédure sont effectuées sur le système sur lequel l'Interface graphique de Data Protection for VMware vSphere est installée.

Conseil : Cette tâche peut également être effectuée à l'aide de l'assistant de configuration ou du bloc-notes de configuration de l'Interface graphique de Data Protection for VMware vSphere. Accédez à la fenêtre de l'Interface graphique de Data Protection for VMware vSphere Configuration et cliquez sur **Lancer l'assistant de configuration** ou sur **Modifier la configuration**.

Procédure

1. Mettez à jour le profil avec les paramètres suivants :

   VE_TSMCLI_NODE_NAME
   Spécifiez le noeud qui connecte l'Interface de ligne de commande Data Protection for VMware au serveur IBM Spectrum Protect et au noeud d'agent (`MY_VMCLINODE`).

   Restriction : Le noeud VMCLI ne prend pas en charge le protocole SSL ou l'authentification LDAP lorsqu'il communique avec le serveur IBM Spectrum Protect.

   VE_VCENTER_NODE_NAME
   Spécifiez le noeud virtuel qui représente un vCenter (`MY_VCNODE`).

   VE_DATACENTER_NAME
   Spécifiez le noeud virtuel qui effectue le mappage vers un centre de données. La syntaxe correcte est la suivante :
   `nom_centre_données::nom_noeud_centre_données`
   - La valeur `nom_centre_données` est sensible à la casse.
   - Veillez à définir ce paramètre pour chaque centre de données de votre environnement (`MY_DCNODE`).
   - L'Interface graphique de Data Protection for VMware vSphere ne prend pas en charge les centres de données de même nom dans vCenter.

VE_TSM_SERVER_NAME
Spécifiez le nom d'hôte ou le protocole IP du serveur IBM Spectrum Protect.

VE_TSM_SERVER_PORT
Indiquez le nom du port à utiliser pour le serveur IBM Spectrum Protect. La valeur par défaut est 1500.

Voici un exemple de profil avec ces paramètres :

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

2. Définissez le mot de passe du noeud VMCLI dans le fichier pwd.txt.
Ce mot de passe est destiné au noeud qui connecte l'Interface de ligne de commande Data Protection for VMware au serveur IBM Spectrum Protect et au noeud de dispositif de transfert de données. Il est défini par le paramètre de profil VE_TSMCLI_NODE_NAME.
   a. Exécutez la commande echo pour créer un fichier texte contenant le mot de passe :

      Linux `echo password1 > pwd.txt`

      Windows `echo password1> pwd.txt`

      Windows Il ne doit pas y avoir d'espace entre le mot de passe (password1) et le signe supérieur à (>).
   b. Exécutez cette commande vmcli pour définir le mot de passe du noeud VMCLI :
      `vmcli -f set_password -I pwd.txt`

      Important :

      - Linux Vous devez exécuter la commande `vmcli -f set_password` en tant qu'utilisateur tdpvmware et non en tant que superutilisateur.
      - Linux Windows Si vous envisagez de générer des rapports de protection des applications, vous devez spécifier le paramètre **-type VMGuest** pour indiquer que le mot de passe s'applique à une machine virtuelle. Par exemple :

        ```
        vmcli -f set_password -type VMGuest -I password.txt
        ```

3. Vérifiez que l'Interface de ligne de commande Data Protection for VMware est en cours d'exécution :

   Windows Cliquez sur **Démarrer** > **Panneau de configuration** > **Outils d'administration** > **Services** et vérifiez que l'état de l'Interface de ligne de commande Data Protection for VMware est Démarré.

   Linux Accédez au répertoire des scripts (/opt/tivoli/tsm/tdpvmware/common/scripts/) et exécutez la commande suivante :

   ```
   ./vmclid status
   ```

   - Si le démon est en cours d'exécution, passez à l'étape 4.
   - Si le démon n'est pas en cours d'exécution, exécutez la commande suivante pour le démarrer manuellement :

     ```
     /opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
     ```

Ces scripts init peuvent également être utilisés pour arrêter et démarrer le démon :

```
./vmclid stop
./vmclid start
```

4. Exécutez la commande vmcli suivante pour vérifier que l'Interface de ligne de commande Data Protection for VMware reconnaît la configuration du noeud IBM Spectrum Protect :

   ```
   vmcli -f inquire_config -t TSM
   ```

5. Validez les noeuds pour confirmer qu'aucune erreur de configuration ne s'est produite :
   a. Démarrez l'Interface graphique de Data Protection for VMware vSphere en cliquant sur l'icône correspondante de la fenêtre Solutions et applications du client vSphere.
   b. Accédez à la fenêtre Configuration.
   c. Sélectionnez un noeud dans le tableau et cliquez sur**Valider le noeud sélectionné**. Des informations d'état s'affichent dans le panneau Détails de l'état.

Que faire ensuite

Linux Windows Vous avez exécuté les trois tâches de configuration manuelles décrites dans cette section :

1. «Configuration des noeuds IBM Spectrum Protect dans un environnement vSphere», à la page 94
2. «Configuration de noeuds de dispositif de transfert de données avec l'interface graphique du plug-in vSphere», à la page 95

Aucune tâche de configuration supplémentaire n'est requise pour sauvegarder vos données de machine virtuelle.

Liste de contrôle de la configuration de l'interface de ligne de commande dans un environnement vSphere

Suivez cette procédure pour configurer Data Protection for VMware dans un environnement vSphere à l'aide d'une interface de ligne de commande uniquement :

Procédure

Exécutez les étapes 1 et 2 sur le serveur IBM Spectrum Protect.

1. Enregistrez les noeuds suivants auprès du serveur IBM Spectrum Protect :
   a. Le noeud qui représente le serveur VMware vCenter (noeud vCenter) :

      ```
      REGister Node MY_VCNODE <mot de passe de MY_VCNODE>
      ```

   b. Le noeud qui communique entre IBM Spectrum Protect et l'Interface graphique de Data Protection for VMware vSphere (noeud VMCLI) :

      ```
      REGister Node MY_VMCLINODE <mot de passe de MY_VMCLINODE>
      ```

   c. Le noeud qui représente le centre de données et dans lequel les données de la machine virtuelle sont stockées (noeud du centre de données) :

      ```
      REGister Node MY_DCNODE <mot de passe de MY_DCNODE>
      ```

   d. Le noeud qui "déplace les données" d'un système à un autre (noeud de dispositif de transfert de données) :

      ```
      REGister Node MY_DMNODE <mot de passe de MY_DMNODE>
      ```

2. Définissez les relations de proxy pour ces noeuds :
   a. Accordez un droit de proxy au noeud vCenter en exécutant la commande suivante :

      ```
      GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
      ```

      Cette commande accorde à MY_DCNODE et à MY_VMCLINODE les droits nécessaires pour sauvegarder et restaurer des machines virtuelles pour le compte de MY_VCNODE.
   b. Accordez un droit de proxy au noeud du centre de données en exécutant la commande suivante :

      ```
      GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
      ```

      Cette commande accorde à MY_VMCLINODE et à MY_DMNODE les droits nécessaires pour sauvegarder et restaurer des machines virtuelles pour le compte de MY_DCNODE.
   c. (Facultatif) Accordez les droits en tant que proxy à tout autre noeud du centre de données ou noeud de dispositif de transfert de données de votre environnement.
   d. Vérifiez les relations de proxy en exécutant la commande Query PROXynode du serveur IBM Spectrum Protect. Le résultat attendu est le suivant :

      ```
      Noeud cible      Noeud d'agent
      --------------   ------------------------------
      MY_VCNODE              MY_DCNODE  MY_VMCLINODE
      MY_DCNODE            MY_VMCLINODE  MY_DMNODE
      ```

Exécutez les étapes 3 à 9 sur le serveur de sauvegarde vStorage.

3. Donnez les valeurs appropriées aux options suivantes du dispositif de transfert de données :
   - Windows Spécifiez ces options dans le fichier d'options dsm.opt.
   - Linux Spécifiez ces options dans le fichier dsm.sys, dans la section concernant le noeud de dispositif de transfert de données.

   ```
   NODENAME
   PASSWORDACCESS
   VMCHOST
   VMBACKUPTYPE
   MANAGEDSERVICES
   TCPSERVERADDRESS
   TCPPORT
   COMMMETHOD
   HTTPPORT
   ```

   Remarque : Le paramètre HTTPPORT est requis lorsque plusieurs services d'accepteur client (CAD) sont utilisés. Par exemple, s'il existe deux noeuds de dispositif de transfert de données (et deux services CAD), le fichier d'options de chaque noeud de dispositif de transfert de données doit spécifier une valeur HTTPPORT différente.
   Voici un exemple de fichier dsm.dm.opt file contenant ces options :

```
NODename MY_DMNODE
PASSWORDAccess            generate
VMCHost vcenter.storage.usca.example.com
VMBACKUPType FUllvm
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.mycompany.xyz.com
TCPPort                   1500
COMMMethod tcpip
HTTPPORT 1583
```

4. Vérifiez la connexion au serveur IBM Spectrum Protect en exécutant la commande suivante :
   `dsmc query session`
5. Lancez la commande suivante pour définir le nom d'utilisateur et le mot de passe VMware vCenter associés au noeud de dispositif de transfert de données :
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`
6. Configurez les services IBM Spectrum Protect suivants :
   - Windows
     a. Installez le service du planificateur :
        ```
        dsmcutil install scheduler /name:"TSM Central Scheduler Service"
        /node:MY_DMNODE   /password:MY_DMNODEPWD /startnow:no /autostart:no
        ```
     b. Installez le service CAD :
        ```
        dsmcutil install cad /name:"TSM CAD - MY_DMNODE" /node:MY_DMNODE
        /password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
        /cadschedname:"TSM Central Scheduler Service" /startnow:no /autostart:yes
        ```
     c. Installez le service d'agent du client distant :
        ```
        dsmcutil install remoteagent /name:"TSM AGENT" /node:MY_DMNODE
        /password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
        /partnername:"TSM CAD - MY_DMNODE" /startnow:no
        ```
   - Linux Spécifiez l'option `managedservices` dans le fichier `dsm.sys`, dans la section correspondant au noeud de dispositif de transfert de données :
     Veillez à spécifier les paramètres `schedule` et `webclient` :
     ```
     managedservices schedule webclient
     ```
     Ce paramètre ordonne à l'accepteur client de gérer à la fois le client Web et le planificateur.
7. Linux Pour configurer le service d'accepteur client et le service du planificateur de transfert de données pour qu'ils fonctionnent comme un serveur de sauvegarde vStorage, vous devez définir la variable d'environnement suivante dans le fichier `/etc/init.d/dsmcad` :
   ```
   export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
   ```
8. Linux Démarrez le service d'accepteur client : Le programme d'installation crée un script de démarrage pour le démon Client Acceptor (`dsmcad`) dans `/etc/init.d`. Pour pouvoir gérer les tâches du planificateur ou le client Web, le démon Client Acceptor doit avoir démarré. En tant que superutilisateur, démarrez le démon à l'aide de la commande suivante :
   ```
   service dsmcad start
   ```
   Pour permettre au démon Client Acceptor de démarrer automatiquement après un redémarrage du système, ajoutez ce service comme suit à l'invite shell :

```
# chkconfig --add dsmcad
```

9. Vérifiez que les services IBM Spectrum Protect sont configurés correctement :
   a. Connectez-vous à un système distant.
   b. Utilisez un navigateur Web pour vous connecter au système `HOST1` à l'aide de cette adresse et de ce port :
   `http://HOST1.xyz.yourcompany.com:1581`

Exécutez l'étape 10 sur le système sur lequel l'Interface graphique de Data Protection for VMware vSphere est installée.

10. Définissez les valeurs appropriées pour les options suivantes dans le profil de l'Interface de ligne de commande Data Protection for VMware (`vmcliprofile`) :

```
VE_TSMCLI_NODE_NAME
VE_VCENTER_NODE_NAME
VE_DATACENTER_NAME
VE_TSM_SERVER_NAME
VE_TSM_SERVER_PORT
```

Voici un exemple de profil avec ces options :

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

Le profil se trouve dans les répertoires suivants :

Linux `/opt/tivoli/tsm/tdpvmware/common/scripts`

Windows 64 bits : `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts`

a. Définissez le mot de passe du noeud VMCLI :
   1) Exécutez la commande `echo` pour créer un fichier texte contenant le mot de passe :

      Linux

      ```
      echo password1 > pwd.txt
      ```

      Windows

      ```
      echo password1> pwd.txt
      ```

   2) Exécutez cette commande vmcli pour définir le mot de passe du noeud VMCLI :

      Important : Linux Vous devez émettre cette commande en tant qu'utilisateur tdpvmware et non en tant que superutilisateur.

      ```
      vmcli -f set_password -I pwd.txt
      ```

b. Vérifiez que l'Interface de ligne de commande Data Protection for VMware est en cours d'exécution :

   Windows Exécutez cette commande à partir d'une invite de commande Windows :
   `net start`

   Linux Exécutez la commande suivante :
   `./vmclid status`

c. Exécutez la commande vmcli suivante pour vérifier que l'Interface de ligne de commande Data Protection for VMware reconnaît la configuration du noeud IBM Spectrum Protect :

```
vmcli -f inquire_config -t TSM
```

Instructions de configuration d'une bande magnétique

Consultez ces instructions avant de tenter une opération de sauvegarde sur la bande magnétique de stockage.

Préparation à la sauvegarde sur bande

Linux Windows Avant de tenter une sauvegarde sur une bande magnétique, ces paramètres doivent être définis sur le serveur IBM Spectrum Protect pour vos sauvegardes de bande magnétique :

1. Définissez la classe de gestion :

   ```
   define mgmtclass <domain name> <policy set name> <mgmtclass name>
   ```

   Par exemple :

   ```
   define mgmtclass tape tape DISK
   ```

2. Définissez le groupe de copie :

   ```
   define copygroup <domain name> <policy set name> <mgmtclass name>
   destination=<stgpool name>
   ```

   Par exemple :

   ```
   define copygroup tape tape DISK destination=Diskpool
   ```

3. Activez l'ensemble de règles :

   ```
   activate policyset <domain name> <policy set name>
   ```

   Par exemple :

   ```
   activate policyset tape tape
   ```

Lorsque vous configurez une sauvegarde sur une bande magnétique physique, des exigences de configuration supplémentaire s'appliquent. Conservez toujours les métadonnées (fichiers de contrôle) IBM Spectrum Protect sur disque et les données de sauvegarde de machine virtuelle réelles sur bande magnétique.

- L'option VMMC permet de stocker les sauvegardes VMware (et les fichiers de contrôle VMware) avec une classe de gestion différente de la classe de gestion par défaut.
- L'option VMCTLMC permet de spécifier la classe de gestion à utiliser spécialement pour les fichiers de contrôle VMware au cours des sauvegardes VMware. La classe de gestion que vous spécifiez remplace la classe de gestion par défaut. Elle remplace également la classe de gestion spécifiée par l'option VMMC. La classe de gestion VMCTLMC doit spécifier un pool de stockage sur disque, sans migration vers la bande.
- L'option VMMC est toujours utilisée pour contrôler la conservation des sauvegardes de machine virtuelle. Cette option s'applique aux configurations sur disque et sur bande magnétique. L'option VMCTLMC n'est pas utilisée pour la conservation des fichiers de contrôle. Les fichiers de contrôle et de données font

partie du même groupement. Ils expirent tous les deux en fonction de la règle de conservation de l'option VMMC. Lorsque les deux options sont définies, VMMC est utilisé pour les fichiers de données et VMCTLMC pour les fichiers de contrôle.

Restriction : Les opérations de restauration qui utilisent des agents de stockage dans les configurations hors réseau local peuvent restaurer les fichiers d'un pool de stockage de copie même si les données sont récupérables à partir d'un pool de stockage principal. Cela peut se produire si la demande de restauration concerne un fichier spécifique ou si cette demande n'utilise pas la méthode sans requête et que la copie principale du fichier est stockée dans un pool de stockage non accessible via un chemin hors réseau local. Cela peut également affecter des situations sans restauration telles que les opérations de sauvegarde Data Protection for VMware. Dans un environnement Data Protection for VMware, le mode de stockage préféré pour les fichiers de contrôle de la machine virtuelle est la sauvegarde sur disque, si bien qu'aucun montage n'est nécessaire pour restaurer le fichier lors du processus de sauvegarde incrémentielle. Non seulement ces fichiers de contrôle doivent être placés sur un disque, mais ils ne doivent pas être sauvegardés sur un pool de stockage de copie accessible via un chemin hors réseau local. S'ils le sont, un montage de bande sera utilisé pour restaurer les fichiers lors d'une sauvegarde incrémentielle hors réseau local à partir du client Data Protection for VMware.

Si l'environnement de serveur IBM Spectrum Protect utilise une migration disque vers bande magnétique, suivez les recommandations suivantes avant la migration :

- Définissez le pool de stockage sur disque MIGDELAY sur une valeur prenant en charge la plupart des demandes de montage à effectuer à partir du disque. Les historiques d'utilisation standard indiquent un pourcentage élevé de récupération de fichiers individuels en quelques jours. Généralement, cela prend entre 3 et 5 jours à partir de la dernière date de modification d'un fichier. Par conséquent, il convient de conserver des données sur disque pendant cette courte période afin d'optimiser les opérations de récupération.

  En outre, si le dédoublonnage côté client est utilisé avec le pool de stockage sur disque, définissez l'option MIGDELAY qui permet des sauvegardes intégrales de machine virtuelle fréquentes. N'effectuez pas la migration du pool de stockage dédoublonné vers la bande magnétique tant qu'au moins deux sauvegardes intégrales n'ont pas été effectuées pour une machine virtuelle. Lorsque des données sont déplacées vers la bande, elles ne sont plus dédoublonnées. Par exemple, si des sauvegardes intégrales sont effectuées chaque semaine, définissez l'option MIGDELAY sur une valeur de 10 jours minimum. Ainsi, vous vous assurez que chaque sauvegarde intégrale identifie et utilise les données dupliquées à partir de la sauvegarde précédente avant de les déplacer sur la bande magnétique.
- Utilisez un pool de stockage de classe d'unités fichier plutôt qu'un pool de stockage de classe d'unités disque. Généralement, la valeur à définir pour la taille de volume (spécifiée par le paramètre de classe d'unités MAXCAPACITY) se situe entre 8 Go et 16 Go. Pour le pool de stockage associé, il est recommandé d'appliquer la colocalisation par espace fichier. Chaque machine virtuelle sauvegardée est représentée en tant qu'espace fichier distinct sur le serveur IBM Spectrum Protect. Le regroupement par espace fichier sauvegarde les données de plusieurs sauvegardes incrémentielles pour une machine virtuelle donnée du même volume (fichier disque). Lors de la migration sur bande magnétique, le regroupement par espace fichier rassemble plusieurs sauvegardes incrémentielles pour une machine virtuelle donnée sur une bande physique.

Utilisez la boîte de dialogue **Paramètres** pour définir la valeur du mode Bande.

Une opération de sauvegarde s'interrompt lorsqu'une opération de montage ou de restauration instantanée requiert le même stockage de bande magnétique simultanément utilisé par l'opération de sauvegarde.

Configuration manuelle d'une unité iSCSI sur un système Linux

Linux

Cette procédure décrit comment configurer un système Linux utilisé lors d'une opération de montage iSCSI. L'image instantanée de la machine virtuelle est montée à partir de l'espace de stockage du serveur IBM Spectrum Protect.

Avant de commencer

Lors d'un montage iSCSI, une cible iSCSI est créée sur le système Recovery Agent. L'initiateur Microsoft iSCSI n'est pas requis sur le système Recovery Agent.

Conseil : L'initiateur Open-iSCSI est fourni avec Red Hat Enterprise Linux et SUSE Linux Enterprise Server.

Prenez connaissance des conditions requises par iSCSI avant de poursuivre cette tâche :

- Vous pouvez vous connecter à la cible iSCSI à partir de n'importe quel système pour créer un volume contenant les données de sauvegarde. Ce volume peut également être monté à partir d'un autre système.
- Un initiateur iSCSI est requis sur tout système devant se connecter à la cible iSCSI.
- Un initiateur iSCSI doit être installé sur le système sur lequel les données doivent être restaurées.
- Si un volume occupe plusieurs disques, vous devez monter tous les disques requis. Lorsque des volumes en miroir sont utilisés, montez uniquement l'un des disques en miroir. Le montage d'un disque évite une opération de synchronisation longue.

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour configurer le système Linux utilisé lors d'une opération de montage iSCSI :

Procédure

1. Enregistrez le nom de l'initiateur iSCSI sur le système sur lequel les données doivent être restaurées. Le nom de l'initiateur iSCSI se trouve dans le fichier `/etc/iscsi/initiatorname.iscsi`. Si la valeur `InitiatorName=` est vide, créez un nom d'initiateur à l'aide de la commande suivante :

   ```
   twauslbkpoc01:~ # /sbin/iscsi-iname
   ```

   Voici un exemple de nom d'initiateur :

   ```
   iqn.2005-03.org.open-iscsi:3f5058b1d0a0
   ```

2. Ajoutez le nom d'initiateur au fichier `/etc/iscsi/initiatorname.iscsi`.
   a. Editez le fichier `/etc/iscsi/initiatorname.iscsi` avec la commande **vi**. Par exemple :

```
twauslbkpoc01:~ # vi /etc/iscsi/initiatorname.iscsi
```

b. Mettez à jour le paramètre **InitiatorName=** avec le nom d'initiateur. Par exemple :

```
InitiatorName=iqn.2005-03.org.open-iscsi:3f5058b1d0a0
```

3. Exécutez les étapes ci-après sur le système où Recovery Agent (ou la cible iSCSI) est installé :
   a. Démarrez Recovery Agent. Renseignez les boîtes de dialogue `Sélectionner un serveur IBM Spectrum Protect` et `Sélectionner un instantané`, puis cliquez sur **Monter**.
   b. Dans la boîte de dialogue `Choisir une destination pour le montage`, sélectionnez `Monter en tant que cible iSCSI`.
   c. Créez un nom de cible. Assurez-vous qu'il est unique et que vous pouvez l'identifier à partir du système qui exécute l'initiateur iSCSI. Par exemple :

      ```
      iscsi-mount-tsm4ve
      ```

   d. Saisissez le nom d'initiateur iSCSI enregistré à l'étape 1 et cliquez sur **OK**.
   e. Vérifiez que le volume que vous venez de monter est affiché dans la zone `Volumes montés`.
4. Localisez et démarrez le programme d'initiateur iSCSI sur le système initiateur sélectionné à l'étape 1 :
   a. Vérifiez que le service iSCSI est en cours d'exécution en lançant la commande suivante :
      Red Hat Enterprise Linux :

      ```
      service iscsi status
      ```

      SUSE Linux Enterprise Server :

      ```
      service open-iscsi status
      ```

      Si le service n'est pas en cours d'exécution, émettez la commande suivante pour le démarrer :
      Red Hat Enterprise Linux :

      ```
      service iscsi start
      ```

      SUSE Linux Enterprise Server :

      ```
      service open-iscsi start
      ```

   b. Connectez-vous à la cible iSCSI en lançant la commande suivante :

      ```
      iscsiadm -m discovery -t sendtargets -p <IP/nom d'hôte du système
      Recovery Agent  system> --login
      ```

   c. Vérifiez qu'une nouvelle unité en mode brut est disponible en lançant la commande suivante :

      ```
      fdisk -l
      ```

5. Montez le système de fichiers :
   En cas de volume non LVM, lancez les commandes suivantes. Dans cet exemple, la nouvelle unité est `/dev/sdb1` :

   ```
   mkdir /mountdir
   mount /dev/sdb1 /mountdir
   ```

   Dans le cas d'un volume LVM, procédez comme suit sur l'invité Linux :
   a. Vérifiez que le script `vgimportclone` est disponible sur le système Linux. Ce script n'est pas fourni dans le package LVM de base (par défaut). Vous devez donc mettre à jour ce dernier vers un niveau fournissant ce script.

b. Lancez la commande **vgimportclone** et incluez un nouveau nom de groupe de volume de base (`VolGroupSnap01`). Par exemple :

```
vgimportclone --basevgname /dev/VolGroupSnap01 /dev/sdb1
```

c. Lancez la commande **lvchange** pour marquer le volume logique comme actif. Par exemple :

```
lvchange -a y /dev/VolGroupSnap01/LogVol00
```

d. Lancez les commandes suivantes pour monter le volume :

```
mkdir /mountdir
mount -o ro /dev/VolGroupSnap01/LogVol00 /mountdir
```

6. Une fois l'opération de restauration de fichier terminée, exécutez les commandes suivantes :
   - En cas de volume non LVM, lancez les commandes suivantes :
     a. Démontage du système de fichiers :

```
umount /dev/sdb1 /mountdir
```

     b. Suppression du volume. Si le volume fait partie d'un groupe de volumes, supprimez d'abord le volume du groupe de volumes à l'aide de la commande suivante :

```
vgreduce <votre_groupe_de_volume> /dev/sdb1
```

        Lancez ensuite la commande suivante pour supprimer le volume :

```
pvremove /dev/sdb1
```

     c. Déconnexion d'une cible unique :

```
iscsiadm --mode node --targetname <target_name> --logout
```

     d. Déconnexion de toutes les cibles :

```
iscsiadm --mode node --logout
```

   - Dans le cas d'un volume LVM, procédez comme suit sur l'invité Linux :
     a. Démontage du système de fichiers :

```
unmount /mountdir
```

     b. Suppression du volume logique :

```
lvm lvremove LogVol00
```

     c. Suppression du groupe de volumes :

```
lvm vgremove VolGroupSnap01
```

     d. Déconnexion d'une cible unique :

```
iscsiadm --mode node --targetname <target_name> --logout
```

     e. Déconnexion de toutes les cibles :

```
iscsiadm --mode node --logout
```

Configuration manuelle d'une unité iSCSI sur un système Windows

Windows

Cette procédure décrit comment configurer un système Windows utilisé lors d'une opération de montage iSCSI. L'image instantanée est montée à partir de l'espace de stockage du serveur IBM Spectrum Protect.

Avant de commencer

Tenez compte des conditions requises par iSCSI avant de poursuivre cette tâche :

- Lors d'un montage iSCSI, une cible iSCSI est créée sur le système Recovery Agent. Vous pouvez vous connecter à la cible iSCSI à partir de n'importe quel

système pour créer un volume contenant les données de sauvegarde. Vous pouvez également monter ce volume à partir d'un autre système.

- L'initiateur iSCSI est requis sur tout système devant se connecter à la cible iSCSI.
- Vérifiez qu'un initiateur iSCSI est installé sur le système sur lequel les données doivent être restaurées.
- L'initiateur Microsoft iSCSI n'est pas requis sur le système Recovery Agent.

Tenez compte des conditions requises pour les disques et les volumes avant de poursuivre cette tâche :

- Si un volume occupe plusieurs disques, vous devez monter tous les disques requis. Lorsque des volumes en miroir sont utilisés, montez uniquement l'un des disques en miroir. Le montage d'un disque évite une opération de synchronisation longue.
- Si plusieurs disques dynamiques ont été utilisés sur le système de sauvegarde, ces disques sont affectés au même groupe. Par conséquent, Windows Disk Manager peut considérer que certains disques sont manquants et émettre un message d'erreur lorsque vous ne montez qu'un seul disque. Ignorez ce message. Les données du disque sauvegardé sont toujours accessibles, sauf si certaines données se trouvent sur un autre disque. Ce problème peut être résolu par le montage de tous les disques dynamiques.

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour configurer le système Windows utilisé lors d'une opération de montage iSCSI :

Procédure

1. Sur le système Recovery Agent, ouvrez le port `3260` dans le pare-feu du réseau local et dans le pare-feu client Windows. Enregistrez le nom de l'initiateur iSCSI sur le système sur lequel les données doivent être restaurées.

   Ce nom est indiqué dans la fenêtre de configuration de l'initiateur iSCSI dans le Panneau de configuration. Par exemple :

   ```
   iqn.1991-05.com.microsoft:hostname
   ```

2. Exécutez ces tâches sur le système où Recovery Agent (ou la cible iSCSI) est installé :

   a. Lancez l'interface graphique de Recovery Agent. Renseignez les boîtes de dialogue Sélectionner un serveur IBM Spectrum Protect et Sélectionner un instantané, puis cliquez sur **Monter**.

   b. Dans la boîte de dialogue Choisir une destination pour le montage, sélectionnez **Monter en tant que cible iSCSI**.

   c. Créez un nom de cible. Assurez-vous qu'il est unique et que vous pouvez l'identifier à partir du système qui exécute l'initiateur iSCSI. Par exemple :

   ```
   iscsi-mount-tsm4ve
   ```

   d. Saisissez le nom d'initiateur iSCSI enregistré à l'étape 1 et cliquez sur **OK**.

   e. Vérifiez que le volume que vous venez de monter est affiché dans la zone Volumes montés.

   f. Lorsque Recovery Agent est utilisé dans un réseau iSCSI et qu'il n'utilise pas de dispositif de transfert de données, accédez au fichier `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf file` et spécifiez la balise `[IMOUNT]` et le paramètre **`Target IP`** :

```
[IMOUNT config]
Target IP=<Adresse IP de la carte réseau du système
exposant les cibles iSCSI.>
```

Par exemple :

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

Après avoir ajouté ou modifié le paramètre Target IP, redémarrez l'interface graphique de Recovery Agent ou l'interface de ligne de commande de Recovery Agent.

3. Localisez et démarrez le programme d'initiateur iSCSI sur le système initiateur sélectionné à l'étape 1 :
   a. Connectez-vous à la cible iSCSI :
      1) Dans l'onglet Cibles, entrez l'adresse TCP/IP de Recovery Agent (cible iSCSI) utilisée dans l'étape 2 de la boîte de dialogue Cible :. Cliquez sur **Connexion rapide**.
      2) La boîte de dialogue Connexion rapide affiche une cible correspondant au nom de cible indiqué à l'étape 2c. Si elle n'est pas déjà connectée, sélectionnez cette cible et cliquez sur **Se connecter**.
   b. Sur le système initiateur, accédez à **Panneau de configuration** > **Outils d'administration** > **Gestion de l'ordinateur** > **Stockage** > **Gestion des disques**.
      1) Si la cible iSCSI montée est répertoriée comme Type=Foreign, cliquez avec le bouton droit de la souris sur **Disque externe** et sélectionnez **Importer des disques externes**. Groupe de disques externes est sélectionné. Cliquez sur **OK**.
      2) La fenêtre suivante affiche le type, la condition et la taille du disque externe. Cliquez sur **OK** et attendez que le disque soit importé.
      3) Une fois l'importation du disque terminée, appuyez sur **F5** (actualiser). L'image instantanée iSCSI montée est visible et contient la lettre d'unité affectée. Si les lettres d'unité ne sont pas automatiquement affectées, cliquez avec le bouton droit de la souris sur la partition requise et sélectionnez **Modifier les lettres d'unité ou les chemins**. Cliquez sur **Ajouter** et sélectionnez une lettre d'unité.
4. Ouvrez Windows Explorer (ou un autre utilitaire) et accédez à l'image instantanée montée pour une opération de restauration de fichier.
5. Une fois le fichier restauré, effectuez les tâches suivantes :
   a. Déconnectez chaque cible iSCSI à l'aide de la boîte de dialogue Propriétés de l'initiateur iSCSI.
   b. Démontez le volume de l'étape 2 en sélectionnant le volume dans l'interface graphique utilisateur de Recovery Agent et en cliquant sur **Démonter**.

Configuration manuelle des noeuds proxy de montage sur un système Linux

Linux

Effectuez cette tâche pour ajouter un noeud proxy de montage à un système Linux distant.

Avant de commencer

Dans un environnement d'Interface graphique de Data Protection for VMware vSphere standard, une section du fichier `dsm.sys` séparée est utilisée pour chaque noeud proxy de montage. Toutes les étapes de cette procédure s'effectuent à l'aide du dispositif de transfert de données installé sur le serveur de sauvegarde.

Pourquoi et quand exécuter cette tâche

Cette tâche configure le noeuds proxy de montage en mettant à jour les options du dispositif de transfert de données et en vérifiant la connectivité au serveur IBM Spectrum Protect.

Procédure

1. Spécifiez ces options dans le fichier `dsm.sys`, dans la section concernant le noeud proxy de montage.

   NODENAME
   Spécifiez le nom d'un noeud proxy de montage précédemment défini. Les planifications IBM Spectrum Protect sont associées à ce noeud.

   PASSWORDACCESS
   Spécifiez GENERATE afin que le mot de passe soit généré automatiquement (à la place d'une invite utilisateur).

   MANAGEDSERVICES
   Indiquez cette option pour diriger l'accepteur client et gérer à la fois le client Web et le planificateur (`schedule webclient`).

   TCPSERVERADDRESS
   Indiquez l'adresse TCP/IP du serveur IBM Spectrum Protect.

   TCPPORT
   Indiquez l'adresse de port TCP/IP du serveur IBM Spectrum Protect.

   COMMMETHOD
   Indiquez la méthode de communication à utiliser par le serveur IBM Spectrum Protect. Pour les noeuds proxy de montage, vous devez spécifier le protocole TCP/IP comme méthode de communication. Les opérations échouent si une autre méthode est spécifiée.

   HTTPPORT
   Cette option indique une adresse de port TCP/IP et doit uniquement être définie lorsque plusieurs services d'accepteur client (CAD) sont utilisés. Par exemple, s'il existe deux noeuds proxy de montage (et deux services CAD), le fichier d'options de chaque noeud proxy de montage doit indiquer une valeur `HTTPPORT` différente.

   Restriction : N'activez pas l'option Hors réseau local (`ENABLELANFREE YES`) dans le fichier `dsm.sys`. Cette option n'est pas prise en charge pour les noeuds proxy

de montage.
Les paramètres d'un fichier dsm.sys sont fournis ici à titre d'exemple :

```
Servername     tsm_server1
  NODename datacenter1_MP_LNX
  PASSWORDAccess            generate
  MANAGEDServices schedule webclient
  TCPServeraddress tsmserver.myco.com
  TCPPort                   1500
  COMMMethod tcpip
  HTTPPORT 1583
```

2. Lancez cette commande pour définir le nom d'utilisation et le mot de passe VMware vCenter associés au noeud proxy de montage:
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`
3. Lancez une session de ligne de commande du dispositif de transfert de données avec les paramètres `-asnodename` et `-optfile` :
   `dsmc -asnodename=vctr1_datacenter1 -optfile=dsm_MP_LNX.sys`
   Vérifiez qu'après votre connexion initiale, vous n'êtes pas invité à entrer votre mot de passe.

   Avertissement : Afin d'éviter toute défaillance du planificateur IBM Spectrum Protect, vérifiez que l'option `asnodename` n'est pas définie dans la section du fichier `dsm.sys` (Linux). Le planificateur recherche sur le serveur IBM Spectrum Protect les planifications associées à `nodename` (noeud proxy de montage), et non à `asnodename` (noeud du centre de données). Si `asnodename` est défini dans `dsm.sys`, les planifications qui sont associées à `asnodename` (et non à `nodename`) sont interrogées. Par conséquent, les opérations de planification échouent.
4. Vérifiez la connexion au serveur IBM Spectrum Protect en exécutant la commande suivante :
   `dsmc query session`
   Cette commande affiche des informations sur votre session, notamment le nom de noeud en cours, la date et l'heure d'établissement de session, ainsi que des informations sur le serveur et sur la connexion serveur.
5. Configurez le service de l'accepteur Client (CAD) et le service du planificateur de transfert de données en exécutant les tâches suivantes :
   - Spécifiez ces options dans le fichier `dsm.sys`, dans la section du noeud proxy de montage :
     - Spécifiez l'option `managedservices` avec les deux paramètres suivants :

       ```
       managedservices schedule webclient
       ```

       Ce paramètre ordonne à l'accepteur client de gérer à la fois le client Web et le planificateur.
     - Si vous souhaitez envoyer les informations sur les planifications et les erreurs à des fichiers journaux autres que les fichiers par défaut, spécifiez les options `schedlogname` et `errorlogname`. Chaque option doit contenir le chemin d'accès complet au fichier et le nom du fichier où les informations de journal doivent être stockées. Par exemple :

       ```
       schedlogname /vmsched/dsmsched_mp_lnx.log
       errorlogname /vmsched/dsmerror_mp_lnx.log
       ```
   - Pour configurer le service d'accepteur client et le service du planificateur de transfert de données pour qu'ils fonctionnent en tant que serveur de sauvegarde, définissez la variable d'environnement suivante dans le fichier `/etc/init.d/dsmcad` :

     ```
     export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
     ```
   - Démarrez le service d'accepteur client :

Le programme d'installation crée un script de démarrage pour le démon Client Acceptor (`dsmcad`) dans `/etc/init.d`. Pour pouvoir gérer les tâches du planificateur ou le client Web, le démon Client Acceptor doit avoir démarré. En tant que superutilisateur, démarrez le démon à l'aide de la commande suivante :

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
service dsmcad start
```

Pour activer le démarrage automatique du démon Client Acceptor après un redémarrage du système, à l'invite shell, ajoutez le service en procédant comme suit :

```
# chkconfig --add dsmcad
```

6. Vérifiez que l'accepteur client et l'agent sont configurés correctement :
   a. Connectez-vous à un système distant.
   b. Utilisez un navigateur Web pour vous connecter au système `HOST1` à l'aide de cette adresse et de ce port :

      ```
      http://HOST1.xyz.yourcompany.com:1581
      ```

Configuration manuelle des noeuds proxy de montage sur un système Windows distant

Windows

Effectuez cette tâche pour ajouter un noeud proxy de montage à un système Windows distant. Cette tâche est requise lorsque vous souhaitez ajouter un second noeud proxy de montage Windows à votre environnement.

Avant de commencer

Avant d'effectuer cette tâche, vérifiez que le noeud proxy de montage Windows principal est configuré.

Pourquoi et quand exécuter cette tâche

Effectuez les étapes suivantes sur le système du proxy de montage Windows distant :

Procédure

1. Installez les produits suivants sur le système du proxy de montage Windows distant :
   - Recovery Agent
   - Dispositif de transfert de données IBM Spectrum Protect

   Les deux produits sont disponibles dans l'image de téléchargement de IBM Spectrum Protect for Virtual Environments. Des instructions d'installation détaillées sont disponibles sur le site IBM Knowledge Center sous «Installation des composants de Data Protection for VMware sur des systèmes Windows», à la page 25
2. Copiez le contenu du fichier d'options exemple du noeud proxy de montage Windows créé et ajoutez-le au fichier d'options situé sur le système du proxy de montage Windows distant :

a. Sur le système du proxy de montage Windows principal, accédez à la fenêtre Configuration dans l'Interface graphique de Data Protection for VMware vSphere.
b. Cliquez sur **Editer la configuration TSM** dans la liste Tâches. Le chargement du bloc-notes de configuration peut prendre quelques instants.
c. Accédez à la page Paires de noeuds proxy de montage.
d. Dans la colonne Noeud principal du tableau, accédez à l'emplacement temporaire où se trouve le noeud proxy de montage Windows et cliquez sur **Afficher les paramètres**.
e. Copiez le contenu du fichier exemple `dsm.opt` qui s'affiche dans la boîte de dialogue **Paramètres de proxy de montage**.
f. Collez (ou ajoutez) le contenu du fichier exemple `dsm.opt` dans le fichier d'options du système proxy de montage Windows distant. Nommez le fichier d'options à l'aide d'une convention permettant d'identifier son rôle en tant que noeud proxy de montage distant.
Par exemple : `dsm.REMOTE1_MP_WIN.opt`.

Restriction : N'activez pas l'option Hors réseau local (`ENABLELANFREE YES`) dans le fichier d'options. Cette option n'est pas prise en charge pour les noeuds proxy de montage.

3. Lancez la commande suivante du dispositif de transfert de données pour définir le nom d'utilisateur et le mot de passe VMware vCenter associés au noeud proxy de montage :

Conseil : Pour démarrer la ligne de commande dsmc, ouvrez le menu **Démarrer** de Windows et sélectionnez **Programmes→ IBM Spectrum Protect → Ligne de commande du client de sauvegarde**.

```
dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
-optfile=dsm.REMOTE1_MP_WIN.opt
```

4. Vérifiez la connexion au serveur IBM Spectrum Protect en exécutant la commande suivante :

```
dsmc query session -optfile=dsm.REMOTE1_MP_WIN.opt
```

Cette commande affiche des informations sur votre session, notamment le nom de noeud en cours, la date et l'heure d'établissement de session, ainsi que des informations sur le serveur et sur la connexion serveur.

5. Configurez le service de l'accepteur Client (CAD) et le service du planificateur de transfert de données en exécutant ces étapes :
Cette étape utilise l'assistant de configuration de l'interface graphique du client IBM Spectrum Protect pour configurer l'accepteur client et le service de planification. Par défaut, le service d'agent du client distant est également configuré à l'aide de l'assistant. Si vous utilisez l'utilitaire de configuration du service client IBM Spectrum Protect (`dsmcutil`) pour cette tâche, assurez-vous d'installer également le service d'agent du client distant.
Lancez l'assistant de configuration de client IBM Spectrum Protect à partir du menu en accédant à **Utilitaires > Assistant de configuration** :
   a. Sélectionnez `Aide à la configuration du client Web TSM`. Entrez les informations demandées par le système.
      1) Dans l'option `Quand souhaitez-vous démarrer le service ?`, sélectionnez `Automatiquement au démarrage de Windows`.

2) Dans l'option Voulez-vous démarrer le service dès la fin de cet assistant ?, sélectionnez Oui.

Une fois l'opération terminée, revenez à la page d'accueil de l'assistant et passez à l'étape b.

Conseil : Lorsque vous configurez plusieurs noeud proxy de montage sur le même système, vous devez spécifier une valeur de port différente pour chaque instance d'accepteur client.

b. Sélectionnez Aide à la configuration du planificateur de client TSM. Entrez les informations demandées par le système.

1) Lorsque vous saisissez le nom du planificateur, veillez à sélectionner l'option Utiliser le démon Client Acceptor (CAD) pour gérer le planificateur.

2) Dans l'option Quand souhaitez-vous démarrer le service ?, sélectionnez Automatiquement au démarrage de Windows.

3) Dans l'option Voulez-vous démarrer le service dès la fin de cet assistant ?, sélectionnez Oui.

6. Vérifiez que l'accepteur client et l'agent sont configurés correctement. Utilisez un navigateur Web pour vous connecter au système HOST1 à l'aide de cette adresse et de ce port :

   http://HOST1.xyz.yourcompany.com:1581

Configuration manuelle de plusieurs services d'accepteur client sur un système Linux

Dans certaines circonstances, il peut s'avérer judicieux d'utiliser plusieurs services dsmcad sur un unique hôte client Linux.

Pourquoi et quand exécuter cette tâche

Cette tâche permet de configurer plusieurs instances dsmcad pour qu'elles s'exécutent et démarrent automatiquement au démarrage du système :

Procédure

1. Créez deux sections de noeud dans le fichier dsm.sys (par défaut, ce fichier se trouve dans /opt/tivoli/tsm/client/ba/bin/) :

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm.sys
SErvername node1
  COMMMethod               TCPip
  TCPPort                  1500
  TCPServeraddress   localhost
  nodename           node1
  errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node1.log
  schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node1.log
  managedservices    webclient sched
  httpport           1581
  passwordaccess     generate

SErvername node2
  COMMMethod               TCPip
  TCPPort                  1500
  TCPServeraddress   localhost
  nodename           node2
  errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node2.log
  schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node2.log
  managedservices    webclient sched
  httpport           1582
  passwordaccess     generate
```

Conseil : Il peut s'avérer judicieux d'inclure certaines options d'inclusion/d'exclusion pour distinguer ces noeuds. Sinon, les mêmes données peuvent être sauvegardées à l'aide des deux noms de noeud.

2. Créez deux fichiers dsm.opt, un pour chaque noeud (par défaut, ces fichiers se trouvent dans `/opt/tivoli/tsm/client/ba/bin`) :

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

3. Activez `passwordaccess generate` en vous connectant à l'aide des données d'identification pour les deux noeuds :

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

4. Réalisez deux copies du script d'initialisation `rc.dsmcad` par défaut (par défaut, ce script se trouve dans `/opt/tivoli/tsm/client/ba/bin`) :

```
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

5. Editez rc.dsmcad-node1 :
   a. Modifiez cette ligne pour les distributions Red Hat Enterprise Linux :

```
daemon $DSMCAD_BIN
```

   Par la ligne suivante :

```
daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

   b. Modifiez cette ligne pour les distributions SUSE Linux Enterprise Server :

```
startproc $DSMCAD_BIN
```

Par la ligne suivante :

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

6. Editez rc.dsmcad-node2 :
   a. Modifiez cette ligne pour les distributions Red Hat Enterprise Linux :

```
daemon $DSMCAD_BIN
```

   Par la ligne suivante :

```
daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

   b. Modifiez cette ligne pour les distributions SUSE Linux Enterprise Server :

```
startproc $DSMCAD_BIN
```

   Par la ligne suivante :

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

7. Créez de nouveaux liens dans /etc/init.d/ qui pointeront vers les deux nouveaux scripts d'initialisation rc.dsmcad. Ces liens permettent au service d'initialisation Linux de démarrer les services dsmcad lors du démarrage du système :

```
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2 dsmcad-node2
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1 dsmcad-node1
# ls -la dsm*
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node1 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node2 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

8. Enregistrez les deux nouveaux scripts rc à l'aide de la commande **chkconfig** :

```
# chkconfig --add dsmcad-node1
# chkconfig --add dsmcad-node2
```

9. Testez la configuration à l'aide de la commande **service dsmcad start** afin de vous assurer que le chargement et le démarrage des scripts s'effectuent sans problème :

```
# service dsmcad-node1 start
Starting dsmcad-node1:                                     [  OK  ]
# service dsmcad-node2 start
Starting dsmcad-node2:                                     [  OK  ]
# ps -ef | grep dsmcad
root 2689 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 2719 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

   Dans cet exemple, le texte de la commande est placé sur deux lignes pour des raisons de formatage.

10. Redémarrez et vérifiez que les deux instances dsmcad démarrent automatiquement :

```
# ps -ef | grep dsmcad
root 1830 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 1856 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

Dans cet exemple, le texte de la commande est placé sur deux lignes pour des raisons de formatage.

Modification du fichier de configuration VMCLI

Le fichier de configuration VMCLI (`vmcliConfiguration.xml`) contient les paramètres définis pour l'Interface graphique de Data Protection for VMware vSphere.

Lors de la procédure d'installation de Data Protection for VMware, un utilisateur doit spécifier une adresse IP pour le serveur vCenter et indiquer si l'accès à l'interface graphique via un navigateur web est possible ou non. Toutefois, après l'installation, cette adresse IP et la méthode d'accès ne peuvent plus être changées.

Pour modifier ces paramètres, vous pouvez éditer manuellement le fichier de configuration VMCLI (`vmcliConfiguration.xml`). Ce fichier est créé lors de l'installation dans les emplacements suivants :
Sur les systèmes Windows :
`C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI`
Sur les systèmes Linux :
`/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/tsmVmGUI/`

Pour indiquer si vous souhaitez activer l'accès à l'interface graphique via un navigateur Web, entrez l'une des valeurs suivantes dans le paramètre **<enable_direct_start></enable_direct_start>** :

- *yes* L'accès à l'interface graphique via un navigateur Web est possible. Par exemple :

  ```
  <enable_direct_start>yes</enable_direct_start>
  ```

- *no* L'accès à l'interface graphique via un navigateur Web n'est pas possible. Par exemple :

  ```
  <enable_direct_start>no</enable_direct_start>
  ```

Pour utiliser l'interface graphique pour la protection vSphere, spécifiez la valeur suivante dans le paramètre **<mode></mode>** :

- *vcenter* L'interface graphique est utilisée pour la protection vSphere. Par exemple :

  ```
  <mode>vcenter</mode>
  ```

Pour modifier l'adresse IP du serveur vCenter, vérifiez que le paramètre **<mode>vcenter</mode>** est défini, puis spécifiez l'adresse IP dans le paramètre **<vcenter_url><vcenter_url>**. Par exemple :

```
<vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
```

La valeur `https://` doit obligatoirement figurer au début de l'adresse IP du serveur vCenter. La valeur `/sdk` doit obligatoirement figurer à la fin de l'adresse IP du serveur vCenter.

Exemples de fichier `vmcliConfiguration.xml`

Le fichier `vmcliConfiguration.xml` suivant est configuré en vue de la protection vSphere et l'accès à l'interface graphique via un navigateur Web est activé :

```
<?xml version="1.0" encoding="UTF-8"?>
<vmcliAdaptor>
 <VMCLIPath>C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\
</VMCLIPath>
 <interruptDelay>900000</interruptDelay>
 <mode>vcenter</mode>
 <vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
 <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

Annexe B. Migration vers une stratégie de sauvegarde incrémentielle incrémentielle-permanente

Procédez comme suit pour migrer les plannings de sauvegarde, les politiques et les noeud de dispositif de transfert de données existants à utiliser dans une stratégie de sauvegarde incrémentielle permanente.

Avant de commencer

Vous pouvez utiliser la stratégie de sauvegarde intégrale incrémentielle-permanente implémentée dans les versions Data Protection for VMware 6.2 et 6.3. Si vous souhaitez continuer à utiliser la stratégie de sauvegarde intégrale incrémentielle-permanente, il n'est pas nécessaire de modifier la politique ou les plannings. Vous devez vous assurer que vous mettez à niveau uniquement les noeuds de dispositif de transfert de données vers la version 6.4 (ou une version ultérieure), comme décrit dans la procédure suivante. Toutefois, si vous souhaitez en outre utiliser la stratégie de sauvegarde incrémentielle incrémentielle-permanente, vous devez également mettre à jour les planifications et les règles pour les noeuds de dispositif de transfert de données qui passent à cette stratégie de sauvegarde incrémentielle permanente.

Pour migrer les plannings Data Protection for VMware existants vers une stratégie de sauvegarde incrémentielle incrémentielle-permanente, vous devez exécuter les tâches décrites dans cette procédure.

Important :

- Bien que certaines tâches soient discrètes, toutes les applications et tous les composants doivent être mis à niveau afin que la stratégie de sauvegarde incrémentielle incrémentielle-permanente puisse s'appliquer. Cette publication fournit toutes les informations nécessaires pour vous guider dans chacune de ces tâches.
- Plusieurs méthodes permettent d'effectuer l'intégralité du processus de migration. Toutefois, les méthodes décrites ici sont considérées comme efficaces pour les environnements Data Protection for VMware typiques.
- Dans cette procédure, la planification à migrer est une planification qui a été créée à l'aide de l'assistant de sauvegarde de l'Interface graphique de Data Protection for VMware vSphere. Si le planning a été créé manuellement, les mises à jour décrites dans cette procédure doivent également être effectuées manuellement.

Pourquoi et quand exécuter cette tâche

Procédure

1. Mettez à niveau tous les serveurs de sauvegarde vStorage protégeant un même vCenter. Vérifiez que la mise à niveau se termine simultanément pour tous les noeuds de dispositif de transfert de données.
   - Pour effectuer cette mise à niveau, vous devez installer le dispositif de transfert de données IBM Spectrum Protect version 6.4 (ou ultérieure) sur le serveur de sauvegarde vStorage.
   - En tant que tâche discrète, il n'est pas nécessaire d'exécuter les étapes 2 et 3 immédiatement après l'étape 1. Une fois les noeuds de dispositif de transfert

de données mis à niveau, vous pouvez poursuivre la sauvegarde des machines virtuelles dans votre environnement existant. Vous pouvez exécuter ces étapes lorsqu'une opportunité plus pratique se présente.

Conseil : Si votre environnement utilise plusieurs serveurs de sauvegarde vStorage, commencez par mettre à niveau un seul serveur. Vérifiez ensuite qu'il fonctionne correctement avant de mettre à niveau les autres serveurs de sauvegarde vStorage.

2. Mettez à jour les règles de sauvegarde et les plannings de sauvegarde pour mettre en oeuvre les sauvegardes incrémentielles incrémentielles-permanentes : Exécutez les tâches de règles de sauvegarde suivantes sur le serveur IBM Spectrum Protect en émettant les commandes suivantes dans le client de ligne de commande d'administration (`dsmadmc`) :

   a. Créez une classe de gestion pour le domaine et l'ensemble de règles concernés pour vos sauvegardes incrémentielles incrémentielles-permanentes. Dans cet exemple, nous allons créer la classe de gestion `mgmt_ifincr28` pour le domaine `domain1` et le l'ensemble de règles `prodbackups`. Le nom de classe de gestion permet de décrire une stratégie de sauvegarde incrémentielle incrémentielle-permanente contenant 28 versions de sauvegarde :

   ```
   define mgmtclass domain1 prodbackups mgmt_ifincr28
   description="Retain 28 backup versions"
   ```

   b. Créez un groupe de copie de sauvegarde pour vos sauvegardes incrémentielles incrémentielles-permanentes. Cet exemple permet de créer un groupe de copie de sauvegarde standard pour le domaine `domain1`, l'ensemble de règles `prodbackups` et la classe de gestion `mgmt_ifincr28` :

   ```
   define copygroup domain1 prodbackups mgmt_ifincr28 standard type=backup
   ```

   Les entrées `standard type=backup` sont des valeurs par défaut qu'il n'est pas nécessaire de définir. Elles sont incluses dans cet exemple pour illustrer que le nom de groupe de copie est `STANDARD` et que le type de groupe de copie est `backup` (et non `archive`).

   c. Mettez à jour le groupe de copie de sauvegarde avec les paramètres de version, conservation et expiration appropriés :

   A faire : Dans Data Protection for VMware versions 6.2 et 6.3, la version de sauvegarde, la conservation et l'expiration sont basées sur un niveau de granularité de chaîne de sauvegarde. Cette méthode signifie que même si des sauvegardes intégrales incrémentielles-permanentes et incrémentielles incrémentielles-permanentes sont exécutées (dans le cadre de la stratégie de sauvegarde intégrale incrémentielle-permanente 6.2 et 6.3), l'expiration de version tient uniquement compte des sauvegardes intégrales. Dans Data Protection for VMware version 6.4 (ou versions ultérieures), la version de sauvegarde, la conservation et l'expiration sont basées sur un niveau de granularité de sauvegarde unique. Cette méthode signifie que l'expiration de la version tient compte à la fois des sauvegardes intégrales incrémentielles-permanentes et des sauvegardes incrémentielles incrémentielles-permanentes.

   Le paramètre `verexists` définit le nombre maximal de versions de sauvegarde de machine virtuelle à conserver sur le serveur. En cas de dépassement de ce nombre en raison d'une sauvegarde incrémentielle incrémentielle-permanente, le serveur fait expirer la version la plus ancienne existant dans l'espace de stockage du serveur. Cet exemple spécifie `verexists = 28`. Cette valeur signifie que 28 versions de sauvegarde d'une machine virtuelle au maximum sont conservées sur le serveur.

Le paramètre retextra définit le nombre maximal de jours pendant lesquels une version de sauvegarde de machine virtuelle sera conservée. Cette version deviendra ensuite inactive. Cet exemple spécifie retextra = nolimit. Cette valeur signifie que le nombre maximal de versions de sauvegarde de machine virtuelle inactives est conservé indéfiniment. Toutefois, lorsque verexists est spécifié, la valeur nolimit est remplacée par la valeur verexists. Dans cet exemple, 28 versions de sauvegarde de machine virtuelle au maximum sont conservés sur le serveur.

Selon les paramètres décrits dans cette étape, le groupe de copie de sauvegarde est mis à jour comme suit :

```
update copygroup domain1 prodbackups mgmt_ifincr28 verexists=28
retextra=nolimit
```

Dans cet exemple, l'environnement Data Protection for VMware version 6.3 se compose des hôtes et planifications suivants :

- Un cluster ESX (esxcluster) contenant deux hôtes ESX (esxhost1, esxhost2).
- La planification bup_esxcluster_full exécute une sauvegarde intégrale incrémentielle-permanente hebdomadaire de chaque hôte ESX avec le noeud de dispositif de transfert de données dm1.
- La planification bup_esxcluster_incr exécute une sauvegarde incrémentielle incrémentielle-permanente quotidienne de chaque hôte ESX avec le noeud de dispositif de transfert de données dm2.

Exécutez les tâches de planification de sauvegarde suivantes dans l'Interface graphique de Data Protection for VMware vSphere :

a. Démarrez l'Interface graphique de Data Protection for VMware vSphere en cliquant sur l'icône correspondante de la fenêtre Solutions et applications du client vSphere.
b. Dans la fenêtre Initiation, cliquez sur l'onglet **Sauvegarde** pour ouvrir la fenêtre Gestion des planifications de sauvegarde.
c. Localisez la planification de sauvegarde (utilisée pour les sauvegardes intégrales incrémentielles-permanentes ou les sauvegardes incrémentielles) à mettre à jour. Dans cette procédure, la planification intégrale incrémentielle-permanente bup_esxcluster_full est utilisée.
d. Cliquez avec le bouton droit sur la planification et sélectionnez **Propriétés**.
e. Accédez à la page Planification et spécifiez **Incrémentielle** dans la liste déroulante **Stratégie de sauvegarde**.
f. Cliquez sur **OK** pour sauvegarder la mise à jour.
g. Localisez la planification de sauvegarde utilisée pour les sauvegardes incrémentielles incrémentielles-permanentes. Cliquez avec le bouton droit sur la planification et sélectionnez **Supprimer**. La planification intégrale incrémentielle-permanente bup_esxcluster_full ayant été mise à jour vers une planification incrémentielle incrémentielle-permanente, cette planification incrémentielle incrémentielle-permanente n'est plus nécessaire.

3. Vous disposez maintenant d'une planification de sauvegarde incrémentielle incrémentielle-permanente. Vous pouvez donc réduire le nombre de noeuds de dispositif de transfert de données en les regroupant :
Dans cet exemple, deux noeuds de dispositif de transfert de données sont regroupés en un seul.
   a. Sur le serveur de sauvegarde vStorage, ouvrez une invite de commande et accédez au répertoire dans lequel le fichier d'options correspondant à dm1 se trouve.

b. A l'aide d'un éditeur de texte (par exemple le Bloc-notes), mettez à jour ce fichier avec les options suivantes :

   1) Spécifiez `vmmaxparallel` pour contrôler le nombre de machines virtuelles sauvegardées simultanément par `dm1` :

      ```
      vmmaxparallel=2
      ```

      La valeur minimale, qui est aussi la valeur par défaut, est égale à 1. La valeur maximale est égale à 50.

      Conseil : Pour chaque noeud de dispositif de transfert de données supprimé, ajoutez 1 à la valeur `vmmaxparallel`.

      Vous pouvez également spécifier `vmlimitperhost` pour contrôler le nombre de machines virtuelles sauvegardées simultanément par `dm1` à partir du même hôte ESX :

      ```
      vmlimitperhost=1
      ```

      Cette option est utile lorsque vous souhaitez empêcher de surcharger un hôte. La valeur par défaut est 0 (aucune limite). La valeur minimale est 1 et la valeur maximale est 50.

c. Connectez-vous au serveur IBM Spectrum Protect. Utilisez le client de ligne de commande d'administration (`dsmadmc`) pour définir le nombre maximal de sessions simultanées de sauvegarde de machine virtuelle pouvant se connecter au serveur. Par exemple :

   ```
   maxsessions=4
   ```

   La valeur par défaut est 25. La valeur minimale est 2.

4. Vérifiez que les noeuds de dispositif de transfert de données mis à jour fonctionnent correctement :

   a. Démarrez l'Interface graphique de Data Protection for VMware vSphere en cliquant sur l'icône dans la fenêtre Solutions et applications de votre client vSphere.

   b. Dans la fenêtre Initiation, cliquez sur l'onglet Configuration pour afficher la page Etat de la configuration.

   c. Dans la page Etat de la configuration, sélectionnez le serveur vCenter protégé à l'étape 1. Cliquez sur un noeud de dispositif de transfert de données pour afficher les informations d'état dans le panneau Détails de l'état. Lorsqu'un noeud affiche un avertissement ou une erreur, cliquez sur ce noeud et utilisez les informations du panneau Détails de l'état pour résoudre l'incident. Puis, sélectionnez le noeud et cliquez sur **Valider le noeud sélectionné** pour vérifier si l'anomalie est résolue. Cliquez sur Actualiser pour retester tous les noeuds.

Résultats

Lorsque l'exécution de toutes les tâches a abouti, l'environnement est prêt à être utilisé dans une stratégie de sauvegarde incrémentielle incrémentielle-permanente.

Restrictions : après avoir migré des planifications de sauvegarde intégrales incrémentielles-permanentes vers des sauvegardes intégrales incrémentielles-permanentes, tenez compte des restrictions suivantes :

- Il n'est pas possible de reconvertir des planifications migrées en sauvegardes intégrales incrémentielles-permanentes par machine virtuelle (espace fichier).

- L'utilisation d'une version antérieure du dispositif de transfert de données IBM Spectrum Protect sur un espace fichier migré n'est pas prise en charge.
- Lorsqu'un espace fichier contient une ou plusieurs sauvegardes incrémentielles incrémentielles-permanentes, les sauvegardes intégrales incrémentielles-permanentes ne sont pas prises en charge.

Exemple de contrôle de version avec le paramètre `verexists`

Dans cet exemple de migration d'une planification, Data Protection for VMware version 6.3 utilise les deux planifications de sauvegarde suivantes.

- `-mode=full` : une sauvegarde intégrale incrémentielle-permanente hebdomadaire est planifiée (les dimanches) et le nombre maximal de versions de sauvegarde de machine virtuelle à conserver sur le serveur est égal à 4 (`verexists=4`).
- `-mode=incr` : une sauvegarde incrémentielle incrémentielle-permanente quotidienne est planifiée (du lundi au samedi).

Le nombre de sauvegardes effectuées pendant une période de quatre semaines est égal à 28 :

- 4 sauvegardes intégrales incrémentielles-permanentes (une sauvegarde intégrale hebdomadaire multipliée par 4 semaines)
- 24 sauvegardes incrémentielles incrémentielles-permanentes (6 sauvegardes incrémentielles hebdomadaires multipliées par 4 semaines)

Comme Data Protection for VMware version 6.3 tient uniquement compte des sauvegardes intégrales, la valeur `verexists=4` permet de conserver les 28 sauvegardes.

Pour offrir le même niveau de protection avec Data Protection for VMware version 6.4 (ou une version ultérieure) et planifier une stratégie de sauvegarde incrémentielle incrémentielle-permanente, créez la planification suivante :
`-mode=iffull` : une sauvegarde intégrale incrémentielle-permanente est planifiée et le paramètre `verexists` est fixé à 28.
Le nombre de sauvegardes effectuées pendant une période de quatre semaines est égal à 28 :

- Une sauvegarde intégrale incrémentielle-permanente (sauvegarde initiale multipliée par 1 jour)
- 27 sauvegardes incrémentielles incrémentielles-permanentes (sauvegardes incrémentielles permanentes quotidiennes multipliées par 27 jours)

Comme Data Protection for VMware version 6.4 (ou versions ultérieures) tient compte des sauvegardes intégrales incrémentielles-permanentes et incrémentielles incrémentielles-permanentes, la valeur `verexists=28` conserve les 28 sauvegardes.

Annexe C. Fonctions d'accessibilité de la famille de produits IBM Spectrum Protect

Les fonctions d'accessibilité aident les utilisateurs souffrant d'un handicap (comme une mobilité réduite ou une vision limitée) à se servir des contenus des technologies de l'information.

Présentation

La famille de produits IBM Spectrum Protect comprend les fonctions d'accessibilité majeures suivantes :

- Fonctionnement à l'aide du clavier uniquement
- Opérations utilisant un lecteur d'écran

La famille de produits IBM Spectrum Protect utilise la dernière norme W3C, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), pour assurer une conformité avec la section US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) et les instructions Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). Pour bénéficier des fonctions d'accessibilité, servez-vous de la dernière version de votre lecteur d'écran et du dernier navigateur pris en charge par le produit.

La documentation produit d'IBM Knowledge Center est activée pour l'accessibilité. Les fonctions d'accessibilité du centre IBM Knowledge Center sont décrites dans la section Accessibilité de l'aide IBM Knowledge Center (www.ibm.com/support/knowledgecenter/about/releasenotes.html#accessibility).

Navigation au clavier

Ce produit utilise les touches de navigation standard.

Informations d'interface

L'interface utilisateur ne comporte pas de contenu qui clignote 2 à 55 fois par seconde.

Les interfaces utilisateur Web s'appuient sur les feuilles de style en cascade pour rendre correctement le contenu Web et fournir une expérience utilisable. L'application permet aux utilisateurs ayant une vision réduite d'utiliser les paramètres d'affichage du système, dont un mode à fort contraste. Vous pouvez contrôler la taille de la police en utilisant les paramètres de l'unité ou du navigateur Web.

Les interfaces utilisateur Web incluent des repères de navigation WAI-ARIA que vous pouvez utiliser pour vous déplacer rapidement dans les différentes zones fonctionnelles de l'application.

Logiciels fournisseur

La famille de produits IBM Spectrum Protect inclut certains logiciels fournisseur non protégés par le contrat de licence IBM. IBM ne présente pas les fonctions

d'accessibilité de ces produits. Contactez le fournisseur pour obtenir les informations d'accessibilité relatives à ses produits.

Informations connexes sur l'accessibilité

En plus des sites Web standard de support d'assistance d'IBM, un service téléphonique TTY est fourni pour les clients sourds ou malentendants afin qu'ils puissent accéder aux services de support et de vente :

Service TTY
800-IBM-3383 (800-426-3383)
(Amérique du Nord)

Pour plus d'informations sur l'engagement d'IBM en matière d'accessibilité, visitez le site IBM Accessibility (www.ibm.com/able).

Remarques

Le présent document a été développé pour des produits et des services proposés aux Etats-Unis et peut être mis à disposition par IBM dans d'autres langues. Toutefois, il peut être nécessaire de posséder une copie du produit ou de la version du produit dans cette langue pour pouvoir y accéder.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est toutefois de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7 Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Les informations fournies dans ce document sont régulièrement modifiées, ces modifications seront intégrées aux prochaines éditions de la publication. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites ne font pas partie des éléments du produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA (IBM Customer Agreement), des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance présentées ici ont été obtenues dans des conditions de fonctionnement spécifiques. Les résultats peuvent donc varier.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM devra être adressée aux fournisseurs de ces produits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des programmes d'application exemples en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de

distribuer ces programmes exemples sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces programmes exemples n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les programmes exemples sont fournis "EN L'ETAT", sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable des dommages liés à l'utilisation des programmes exemples.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit : © (nom de votre société) (année). Des segments de code sont dérivés des Programmes exemples IBM Corp. © Copyright IBM Corp. _entrer la ou les années_.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Adobe est une marque d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Linear Tape-Open, LTO et Ultrium sont des marques de HP, IBM Corp. et Quantum, aux Etats-Unis et/ou dans certains autres pays.

Intel et Itanium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows et Windows NT sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et dans certains autres pays.

VMware, VMware vCenter Server et VMware vSphere sont des marques de VMware, Inc. ou de ses filiales aux Etats-Unis et dans certains autres pays.

Dispositions relatives à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Applicabilité
Ces dispositions s'ajoutent aux conditions d'utilisation relatives au site Web IBM.

Usage personnel
Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas distribuer ni afficher tout ou partie de ces publications ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

Usage commercial
Vous pouvez reproduire, distribuer et publier ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces publications en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits Excepté les droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des informations s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Politique de confidentialité

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

La présente Offre Logiciels n'utilise pas de cookies ni aucune autre technologie pour collecter des informations personnelles identifiables.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la déclaration IBM de confidentialité sur Internet à l'adresse http://http://www.ibm.com/privacy/fr/fr/, la section “Cookies, pixels espions et autres technologies” de la Déclaration IBM de confidentialité sur Internet à l'adresse http://http://www.ibm.com/privacy/details/fr/fr et la section “IBM Software Products and Software-as-a-Service Privacy Statement” à l'adresse http://www.ibm.com/software/info/product-privacy.

Glossaire

Un glossaire réunissant les termes et définitions qui se rapportent à la famille de produits IBM Spectrum Protect est disponible.

Voir Glossaire IBM Spectrum Protect.

Index

R

S

U

V

W

Numéro de programme : 5725-X00