Guide d'administration de vSphere Data Protection

vSphere Data Protection 5.1

Ce document porte sur la version indiquée de chaque produit répertorié, ainsi que toutes les versions ultérieures, jusqu'à ce qu'il soit remplacé par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur http://www.vmware.com/fr/support/pubs.

FR-000846-00

vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware, à l'adresse suivante :

http://www.vmware.com/fr/support/

Le site Web de VMware propose également les dernières mises à jour des produits.

N'hésitez pas à nous transmettre vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

VMware, Inc.
Tour Franklin, 100-101 Quartier Boieldieu
92042 Paris La Défense
http://www.vmware.fr

Table des matières

À propos de ce guide

Le guide d'administration de vSphere Data Protection explique comment installer et gérer les sauvegardes des PME.

Audience visée

Ce guide s'adresse à quiconque souhaite fournir des solutions de sauvegarde à l'aide de vSphere Data Protection. Les informations qui y figurent s'adressent aux administrateurs confirmés de systèmes Windows ou Linux qui maîtrisent la technologie des machines virtuelles et les opérations de datacenter.

Glossaire de VMware Technical Publications

VMware Technical Publications fournit un glossaire des termes qui ne vous sont peut-être pas familiers. Pour une définition des termes utilisés dans la documentation technique de VMware, rendez-vous sur http://www.vmware.com/fr/support/pubs.

Commentaires sur la documentation

Nous vous invitons à partager votre avis afin d'améliorer notre documentation. Faites part de vos commentaires à l'adresse suivante : docfeedback@vmware.com.

Ressources de support technique et de formation

Les ressources de support technique suivantes sont à votre disposition. Pour accéder à la version actuelle d'autres guides, rendez-vous sur http://www.vmware.com/fr/support/pubs.

Support en ligne

Le support en ligne vous permet de soumettre des demandes de support technique, de consulter les informations concernant vos produits et contrats, et d'enregistrer vos produits. Pour y accéder, rendez-vous sur http://www.vmware.com/fr/support/phone_support.html.

Offres de support

Pour découvrir comment les offres de support VMware peuvent répondre aux besoins de votre entreprise, rendez-vous sur http://www.vmware.com/fr/support/services.

VMware Professional Services

Les cours VMware Education Services proposent des exercices pratiques intensifs, des exemples d'étude de cas, ainsi que de la documentation destinée à servir de référence sur site. Les cours sont disponibles sur site, en salle de formation et en ligne. Pour les programmes pilotes sur site et les bonnes pratiques d'implémentation, VMware Consulting Services propose des offres destinées à vous aider à évaluer, planifier, élaborer et gérer votre environnement virtuel. Pour accéder aux informations sur les cours de formation, les programmes de certification et les services de consulting, rendez-vous sur http://www.vmware.com/fr/services.

Comprendre vSphere Data Protection 1

vSphere Data Protection (VDP) est une solution de sauvegarde et de restauration sur disque fiable et simple à déployer. Entièrement intégrée avec VMware vCenter Server, elle permet une gestion centralisée et efficace des procédures de sauvegarde tout en stockant les sauvegardes dans un système de stockage de destination dédupliqué.

Les avantages de vSphere Data Protection sont les suivants :

- Protection rapide et efficace des données pour l'ensemble de vos machines virtuelles, y compris celles qui sont arrêtées ou qui sont déplacées entre des hôtes physiques
- Réduction considérable de l'espace disque occupé par les données de sauvegarde grâce à une déduplication intelligente appliquée à toutes les sauvegardes
- Baisse du coût de la sauvegarde des machines virtuelles et réduction maximale des fenêtres de sauvegarde grâce au suivi des blocs modifiés et aux snapshots de machine virtuelle VMware
- Permet des sauvegardes simples sans la présence d'agents tiers installés sur chaque machine virtuelle
- Installation très simple de la solution grâce à son intégration avec vSphere et possibilité de la gérer via un portail Web
- Accès direct à la configuration de vSphere Data Protection à partir d'un client Web vSphere standard
- Protection des sauvegardes grâce à des mécanismes de point de contrôle et de retour arrière
- Restauration simplifiée de fichiers Windows et Linux avec des restaurations en mode fichier démarrées par l'utilisateur à partir d'une interface Web

Ce chapitre comporte les rubriques suivantes :

Présentation de vSphere Data Protection

L'interface de VMware vSphere Web Client permet de sélectionner, planifier, configurer et gérer des sauvegardes et des restaurations de machines virtuelles.

Lors d'une sauvegarde, vSphere Data Protection crée un snapshot passif de la machine virtuelle. La déduplication s'effectue automatiquement avec chaque opération de sauvegarde.

Dans le contexte des sauvegardes et restaurations, les termes suivants sont employés dans le présent document.

- Un **datastore** est une représentation virtuelle d'un ensemble de ressources de stockage physiques sous-jacentes dans le datacenter. Un datastore est l'emplacement de stockage (par exemple, un disque physique, un RAID ou un SAN) des fichiers de machine virtuelle.
- **CBT (Changed Block Tracking)** est une fonction de VMkernel qui permet le suivi des blocs de stockage des machines virtuelles à mesure qu'ils évoluent dans le temps. Le VMkernel effectue le suivi des changements de bloc sur les machines virtuelles, ce qui améliore le processus de sauvegarde pour les applications qui ont été développées dans l'optique de tirer parti des API vStorage de VMware.
- **Les VADP (VMware vStorage APIs for Data Protection)** permettent à un logiciel de sauvegarde de réaliser des sauvegardes centralisées de VM sans interruption et sans temps système lié à l'exécution de tâches de sauvegarde à l'intérieur de chaque machine virtuelle.
- **VMDK (Virtual Machine Disk)** désigne un fichier ou ensemble de fichiers qui se présente au système d'exploitation invité sous la forme d'un disque physique. Ces fichiers peuvent se trouver sur la machine hôte ou sur un système de fichiers distant.
- **L'appliance vSphere Data Protection** est une appliance virtuelle conçue pour la protection de données vSphere.

Sauvegarde et restauration en mode image

vSphere Data Protection crée des sauvegardes en mode image qui sont intégrées avec vStorage API for Data Protection, ensemble de fonctionnalités dans vSphere qui permet de décharger le temps système du traitement des sauvegardes depuis la VM vers l'appliance vSphere Data Protection. L'appliance communique avec vCenter Server pour effectuer un snapshot du VMDK des VM. La déduplication a lieu dans l'appliance à l'aide d'une technologie de déduplication à longueur variable brevetée.

Pour prendre en charge les nombreux environnements VMware de grandes dimensions et dont la taille ne cesse d'augmenter, chaque appliance vSphere Data Protection peut sauvegarder simultanément huit machines virtuelles afin d'optimiser la capacité en volume de la protection des données.

Pour améliorer l'efficacité des sauvegardes en mode image, vSphere Data Protection utilise la fonction CBT des VADP. CBT est une fonction VMware qui permet à vSphere Data Protection de sauvegarder uniquement les blocs de disque qui ont changé depuis la dernière sauvegarde. Cela permet de réduire considérablement le temps de sauvegarde d'une image de VM donnée et de traiter un grand nombre de VM dans une fenêtre de sauvegarde particulière.

Grâce au suivi des blocs modifiés (CBT) lors des restaurations, vSphere Data Protection offre des restaurations rapides et efficaces lors du rétablissement de VM à leur emplacement d'origine. Au cours d'une restauration, vSphere Data Protection interroge la VADP pour déterminer les blocs qui ont changé depuis la dernière sauvegarde, puis restaure ou remplace uniquement ces blocs. Cela réduit le transfert de données au sein de l'environnement vSphere lors d'une opération de restauration et, surtout, l'objectif de temps de restauration (RTO).

En outre, vSphere Data Protection évalue automatiquement la charge de travail entre les deux méthodes de restauration (restauration d'image complète ou restauration avec suivi des blocs modifiés CBT) et choisit la méthode qui permettra le temps de restauration le plus court. Cela s'avère très utile lorsque le taux de changement depuis la dernière sauvegarde dans une VM restaurée est très élevé et que le temps système d'une analyse CBT serait moins intéressant que la restauration directe d'une image complète. vSphere Data Protection détermine de façon logique la méthode de déploiement qui permettra d'obtenir les temps de restauration d'image VM les plus courts dans votre situation ou environnement.

Les avantages des sauvegardes d'image VMware sont les suivants :

- Sauvegardes d'image complète de VM, indépendamment du système d'exploitation invité
- Emploi de la méthode efficace de transport SCSI hotadd lorsqu'elle est disponible et qu'elle dispose d'une licence correcte, ce qui évite la copie de l'image intégrale du VMDK sur le réseau
- Restauration en mode fichier à partir de sauvegardes en mode image
- Déduplication entre l'ensemble des fichiers .vmdk protégés par l'appliance vSphere Data Protection
- Utilisation du suivi des blocs modifiés pour des sauvegardes et restaurations plus rapides
- Trafic réseau réduit grâce à la déduplication et à la compression des données
- Absence de gestion d'agents de sauvegarde dans chaque VM
- Prise en charge de la sauvegarde et de la restauration simultanées pour un débit plus élevé

IMPORTANT Pour des sauvegardes d'image VM, la bonne pratique consiste à installer VMware Tools sur chaque machine virtuelle. VMware Tools fournit une fonctionnalité de sauvegarde supplémentaire qui met en veille certains processus sur l'OS invité avant la sauvegarde.

Restauration en mode fichier

La restauration en mode fichier (FLR) permet aux administrateurs locaux de VM protégées de parcourir et de monter des sauvegardes pour la machine locale. À partir de ces sauvegardes montées, l'administrateur peut restaurer des fichiers individuels. La restauration en mode fichier s'effectue à l'aide du client de restauration vSphere Data Protection.

Avantages d'une zone de stockage avec déduplication

Les données d'entreprise sont hautement redondantes avec des fichiers identiques ou des données stockées dans plusieurs systèmes (par exemple, des fichiers ou des documents d'OS envoyés à plusieurs destinataires). Les fichiers modifiés présentent également une redondance élevée avec des versions antérieures. Les méthodes de sauvegarde traditionnelles amplifient cette redondance en stockant constamment l'ensemble de ces données. vSphere Data Protection utilise une technologie de déduplication brevetée pour éliminer cette redondance au niveau du fichier et au niveau des segments de données à l'intérieur du fichier.

Segments de données à longueur variable et à longueur fixe

Dans l'élimination des données redondantes au niveau d'un segment (ou sous-fichier), la méthode permettant de déterminer la taille du segment est un facteur clé. Les segments à bloc ou à longueur fixe sont communément employés par les technologies de snapshot et de déduplication. Malheureusement, même de légères modifications apportées à un dataset (par exemple, l'insertion de données au début d'un fichier) peuvent modifier tous les segments à longueur fixe de ce dataset, alors que ce dernier a très peu changé. vSphere Data Protection utilise une méthode à longueur variable intelligente pour déterminer la taille des segments, qui permet d'examiner les données afin d'identifier les points de limite logique et d'optimiser ainsi l'efficacité.

Détermination logique des segments

vSphere Data Protection recourt à une méthode brevetée pour déterminer la taille des segments et optimiser l'efficacité dans l'ensemble des systèmes. L'algorithme de vSphere Data Protection analyse la structure binaire d'un dataset (tous les 0 et les 1 contenus dans le dataset) afin de déterminer les limites de segments qui sont dépendantes d'un contexte. Les segments à longueur variable font en moyenne 24 Ko, et 12 Ko une fois compressés.

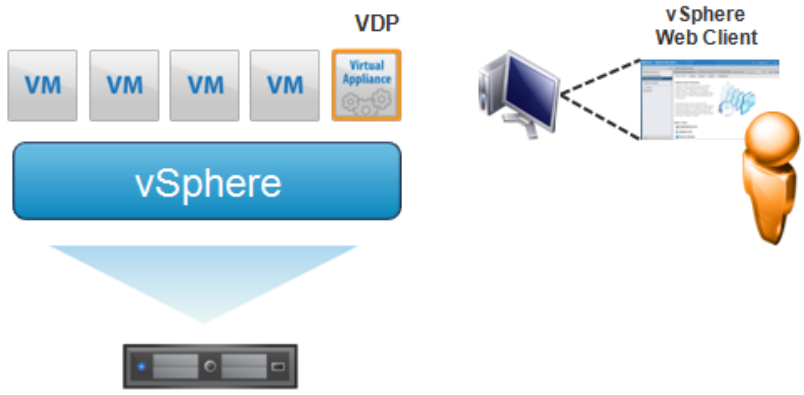
En analysant la structure binaire des fichiers VMDK, vSphere Data Protection fonctionne pour tous les types et tailles de fichier et déduplique les données de manière logique.

Architecture de vSphere Data Protection

vSphere Data Protection (VDP) utilise un client Web vSphere et une appliance vSphere Data Protection pour stocker les sauvegardes dans un système de stockage dédupliqué.

vSphere Data Protection est formé d'un ensemble de composants qui s'exécutent sur différentes machines (voir le schéma suivant).

- vSphere 5.1
- Appliance vSphere Data Protection (installée sur VMware ESX/ESXi 4.x ou 5.x)
- vSphere Web Client.



Installation et configuration de vSphere Data Protection

2

Ce chapitre comporte les rubriques suivantes :

Dimensionnement vSphere Data Protection

Le dimensionnement vSphere Data Protection permet de déterminer la taille des appliances vSphere Data Protection et le nombre d'appliances nécessaires sur la base des critères suivants :

- Nombre et types de VM (la VM contient-elle des données de système de fichiers ou de base de données ?)
- Quantité de données
- Durée de rétention (jours, semaines, mois, années)
- Taux de changement habituel

Le tableau suivant présente des exemples de recommandation de dimensionnement vSphere Data Protection :

Tableau 2-1. Exemples de recommandations pour le dimensionnement vSphere Data Protection

Nombre de machines virtuelles	Stockage de données par client	Rétention : jours	Rétention : semaines	Rétention : mois	Rétention : années	Recommandation
25	20 Go	30	0	0	0	1 VDP de 0,5 To
25	20 Go	30	4	12	7	1 VDP de 2 To
25	40 Go	30	4	12	7	2 VDP de 2 To
50	20 Go	30	0	0	0	1 VDP 1 To
50	20 Go	30	4	12	7	2 VDP de 2 To
50	40 Go	30	4	12	7	3 VDP de 2 To
100	20 Go	30	0	0	0	1 VDP de 2 To
100	20 Go	30	4	12	7	3 VDP de 2 To
100	40 Go	30	4	12	7	6 VDP de 2 To

Les recommandations ci-dessus (données à titre informatif uniquement) sont basées sur les hypothèses suivantes :

- Les VM contiennent principalement des données de système de fichiers. Si les VM contiennent principalement des données de base de données, les taux de déduplication seront plus faibles.
- Taux de déduplication initial de 70 % pour des données de système de fichiers.
- Taux de déduplication quotidien de 99,7 % pour des données de système de fichiers.
- Le taux de croissance annuel est de 5 %.

IMPORTANT En cas de doute sur la taille de l'appliance à déployer, il est préférable d'utiliser un datastore vSphere Data Protection plus volumineux. Une fois qu'une appliance est déployée, la taille du datastore ne peut pas changer.

Configuration logicielle

vSphere Data Protection 5.1 nécessite les logiciels suivants :

- VMware vCenter Server
  - vCenter Server Linux ou Windows : Version 5.1
  - Le vSphere Web Client est pris en charge sur Microsoft Internet Explorer 7 et 8 (des problèmes ont récemment été recensés concernant l'exécution du vSphere Web Client sur IE 8) ou Mozilla Firefox 3.6 ou version ultérieure.
  - Les navigateurs Web doivent prendre en charge Adobe Flash Player 11.3 ou une version ultérieure pour accéder au vSphere Web Client ou aux fonctionalités de vSphere Data Protection.
- VMware ESX/ESXi (les versions suivantes sont prises en charge)
  - 4.0, 4.0i, 4.1i, 5.0i, 5.1
- Version de l'appliance :
  - vSphere Data Protection : 5.1

Configuration matérielle

L'appliance vSphere Data Protection est disponible sous forme de trois options :

- VDP 0,5 To
- VDP 1 To
- VDP 2 To

IMPORTANT Une fois que vSphere Data Protection est déployé, la taille ne peut pas être modifiée.

La configuration matérielle de chaque option de vSphere Data Protection est indiquée dans le tableau suivant.

	VDP 0,5 To	VDP 1 To	VDP 2 To
Processeurs dédiés à vSphere Data Protection	Quatre processeurs 2 GHz au minimum disponibles en permanence pour vSphere Data Protection	Quatre processeurs 2 GHz au minimum disponibles en permanence pour vSphere Data Protection	Quatre processeurs 2 GHz au minimum disponibles en permanence pour vSphere Data Protection
Mémoire physique dédiée à vSphere Data Protection	4 Go	4 Go	4 Go
Espace disque	850 Go	1 600 Go	3 100 Go
Connexion réseau	Connexion 1 GbE	Connexion 1 GbE	Connexion 1 GbE

Spécifications vSphere Data Protection

vSphere Data Protection prend en charge les spécifications suivantes :

- Chaque appliance vSphere Data Protection prend en charge jusqu'à 100 VM
- Chaque vCenter Server peut prendre en charge jusqu'à 10 appliances vSphere Data Protection
- Prise en charge du stockage avec déduplication de 0,5, 1 ou 2 To

Configuration préalable à l'installation

Avant d'installer vSphere Data Protection, DNS et NTP doivent être configurés.

Configuration DNS

Avant de déployer vSphere Data Protection, une entrée doit être ajoutée au serveur DNS pour l'adresse IP de l'appliance et le nom d'hôte complet qualifié (FQDN). Ce serveur DNS doit prendre en charge la résolution des noms et la résolution inverse.

IMPORTANT Si le serveur DNS n'est pas correctement configuré, de nombreux problèmes de configuration ou d'exécution risquent de survenir.

Pour vérifier si le serveur DNS est correctement configuré :

1 Ouvrez une invite de commande et entrez la commande suivante :

nslookup <*adresse_ip_VDP_IP_*> <*adresse_IP_DNS*>

La commande nslookup retournera le nom d'hôte complet qualifié de l'appliance vSphere Data Protection.

2 Entrez la commande suivante :

nslookup <*FQDN_de_VDP*> <*adresse_IP_DNS*>

La commande nslookup retournera l'adresse IP de l'appliance vSphere Data Protection.

3 Si les commandes nslookup ont retourné les informations appropriées, fermez l'invite de commande. Sinon, résolvez la configuration DNS avant d'installer vSphere Data Protection.

Configuration du protocole NTP

vSphere Data Protection utilise le protocole NTP (Network Time Protocol). Avant d'installer vSphere Data Protection, le protocole NTP doit être configuré sur le vCenter Server et l'hôte VMware ESXi sur lequel vSphere Data Protection sera installée.

Reportez-vous à la documentation de VMware ESXi et du vCenter Server pour en savoir plus sur la configuration du protocole NTP.

Configuration des comptes utilisateur

Le compte utilisateur vCenter ou administrateur SSO ne peut être utilisé avec vSphere Data Protection qu'après l'ajout de l'utilisateur correspondant en tant qu'administrateur sur le noeud racine de vCenter. Pour configurer l'utilisateur vSphere Data Protection ou l'utilisateur administrateur SSO à l'aide de vSphere Client, procédez comme suit :

1 Connectez-vous au vSphere Web Client et sélectionnez **vCenter** > **Hôtes et clusters**.

2 Dans le volet de gauche, cliquez sur vCenter Server.

3 Cliquez sur l'onglet **Gérer**, puis sur le sous-onglet **Autorisations**.

4 Cliquez sur l'icône **Ajouter une autorisation**.

5 Cliquez sur **Ajouter**.

6 Dans le menu déroulant Domaine, sélectionnez un domaine, serveur ou SYSTEM-DOMAIN.

7 Sélectionnez l'utilisateur qui sera l'administrateur de vSphere Data Protection ou l'administrateur SSO, puis cliquez sur **Ajouter**.

8 Cliquez sur **OK**.

9 Dans le menu déroulant Rôle attribué, sélectionnez Administrateur.

10 Vérifiez que la case Propager aux objets enfants est sélectionnée.

11 Cliquez sur **OK**.

Pour vérifier que l'utilisateur est répertorié sous Administrateurs, allez à **Accueil > Administration > Gestionnaire de rôles** et cliquez sur le rôle **Administrateur**. L'utilisateur que vous venez d'ajouter doit être répertorié à droite de ce rôle.

IMPORTANT Si l'utilisateur de sauvegarde vSphere Data Protection qui a recours à l'interface VDP-configure appartient à un compte de domaine, il doit être entré dans le format “SYSTEM-DOMAIN\admin” dans vdp-configure. Si le nom d'utilisateur est entré au format “admin@SYSTEM-DOMAIN” , les tâches associées à la procédure de sauvegarde risquent de ne pas s'afficher dans les tâches en cours récentes.

Déployer le modèle OVF

Conditions préalables

- L'appliance vSphere Data Protection doit être installée sur un hôte VMware ESXi 4.0, 4.1, 5.0 ou 5.1.
- vCenter 5.1 est nécessaire. Connectez-vous à vCenter à partir d'un vSphere Web Client pour déployer le modèle OVF.
- L'appliance vSphere Data Protection se connecte à VMware ESXi à l'aide du port 902. S'il existe un pare-feu entre l'appliance et VMware ESXi, le port 902 doit être ouvert.
- Le plug-in VMware Client Integration 5.1.0 doit être installé sur votre navigateur.

Procédure

1. Connectez-vous au vSphere Web Client et sélectionnez **vCenter > Datacenters.**
2. Sous l'onglet Objets, cliquez sur **Actions > Déployer le modèle OVF.**
3. Sélectionnez la source sur laquelle se trouve l'appliance vSphere Data Protection.
4. La source par défaut est Packages OVF. Remplacez-la par **Packages OVA**.
5. Sélectionnez l'appliance et cliquez sur **Ouvrir.**
6. Après avoir sélectionné le fichier .ova de l'appliance, cliquez sur **Suivant**.
7. Passez en revue les détails du modèle et cliquez sur **Suivant**.
8. Sur l'écran d'acceptation du contrat de licence, lisez les conditions du contrat, cliquez sur **Accepter**, puis sur **Suivant**.
9. Sur l'écran de sélection du nom et du dossier, entrez le nom de l'appliance et cliquez sur le dossier ou le datacenter dans lequel vous souhaitez la déployer. Cliquez ensuite sur **Suivant.**
10. Sélectionnez l'hôte de l'appliance, puis cliquez sur **Suivant**.
11. Sélectionnez le format de disque virtuel (« Conséquences du choix de disques provisionnés fins ou épais » à la page 42 fournit des informations supplémentaires) et l'emplacement de stockage de l'appliance. Cliquez sur **Suivant**.
12. Sélectionnez le réseau de destination de l'appliance, puis cliquez sur **Suivant**.
13. Dans le modèle Personnaliser, définissez la **passerelle par défaut, le serveur DNS, l'adresse IP du réseau 1** et son **masque de sous-réseau**. Vérifiez que les adresses IP sont correctes. Si les adresses IP définies dans cette boîte de dialogue sont incorrectes, vous devez redéployer le modèle .ova. Cliquez sur **Suivant**.

REMARQUE L'appliance vSphere Data Protection ne prend pas en charge DHCP. Elle nécessite une adresse IP statique.

14. Sur l'écran Prêt à terminer, vérifiez que toutes les options de déploiement sont correctes et cliquez sur **Terminer**.

vCenter déploie l'appliance vSphere Data Protection. Surveillez les **tâches récentes** pour déterminer si le déploiement est terminé.

Installation et configuration de vSphere Data Protection

Conditions préalables

Le modèle .ovf de vSphere Data Protection (voir « Déployer le modèle OVF » à la page 15) doit avoir été déployé sans erreur, et vous devez être connecté au vCenter Server à partir du vSphere Web Client.

Procédure

1. Sélectionnez **Accueil vCenter > vCenter > VM et modèles**. Développez l'arborescence de vCenter et sélectionnez l'appliance vSphere Data Protection. Cliquez avec le bouton droit de la souris sur l'appliance et sélectionnez **Mise sous tension**.
2. Cliquez avec le bouton droit de la souris sur l'appliance et sélectionnez **Ouvrir la console**.
3. Une fois les fichiers d'installation chargés, l'écran de bienvenue du menu vSphere Data Protection s'affiche. Ouvrez un navigateur Web et saisissez :

   https://<*adresse IP de l'appliance VDP*>:8543/vdp-configure/
4. Sur l'écran Connexion VMware, saisissez les informations suivantes :
   a. Utilisateur : **root**
   b. Mot de passe : **changeme**
   c. Cliquez sur **Connexion**.
5. L'écran de bienvenue s'ouvre. Cliquez sur **Suivant**.
6. La boîte de dialogue Paramètres réseau s'affiche. Définissez (ou confirmez) les paramètres suivants :
   a. Adresse IPv4 statique
   b. Masque de réseau
   c. Passerelle
   d. DNS primaire
   e. DNS secondaire
   f. Nom d'hôte
   g. Domaine
7. Cliquez sur **Suivant**.
8. La boîte de dialogue Fuseau horaire s'affiche. Sélectionnez le fuseau horaire approprié, puis cliquez sur **Suivant**.
9. La boîte de dialogue Informations d'identification vSphere Data Protection s'ouvre. Pour les Informations d'identification de vSphere Data Protection, entrez le mot de passe de l'appliance. Il s'agira du mot de passe de configuration universel. Entrez un mot de passe répondant aux critères suivants :
   - Neuf caractères
   - Au moins 1 caractère en majuscule
   - Au moins 1 caractère en minuscule
   - Au moins un chiffre
   - Aucun caractère spécial
10. Cliquez sur **Suivant**.

11 La boîte de dialogue Gestion des licences vCenter s'affiche. Indiquez les éléments suivants :

   a Nom d'utilisateur vCenter (si l'utilisateur appartient à un compte de domaine, il doit être entré au format “SYSTEM-DOMAIN\admin”)

   b Mot de passe vCenter

   c Nom d'hôte vCenter [adresse IP ou nom d'hôte complet qualifié (FQDN)]

   d Port vCenter

   e Nom d'hôte SSO [adresse IP ou nom d'hôte complet qualifié (FQDN)]

   f Port SSO

12 Cliquez sur **Tester la connexion**.

   Un message de réussite de la connexion s'affiche. Si tel n'est pas le cas, redéfinissez les paramètres et répétez l'étape jusqu'à l'obtention de ce message.

   Si vous recevez le message « L'utilisateur indiqué n'est pas un utilisateur dédié de la VDP ou ne dispose pas des privilèges vCenter suffisants pour administrer la VDP. Mettez à jour votre rôle d'utilisateur et réessayez », reportez-vous aux instructions de la rubrique « Configuration des comptes utilisateur » à la page 14 pour la mise à jour du rôle d'utilisateur.

13 Cliquez sur **OK**.

14 Cliquez sur **Suivant**.

15 La page Prêt à terminer s'ouvre. Cliquez sur **Terminer**.

16 Un message vous indique que la configuration est terminée. Cliquez sur **OK**.

La configuration de l'appliance vSphere Data Protection est désormais terminée, mais vous devez retourner au vSphere Web Client et redémarrer l'appliance. Dans le vSphere Web Client, cliquez avec le bouton droit de la souris sur l'appliance et sélectionnez **Redémarrer l'OS invité**. Dans le message Confirmer le redémarrage, cliquez sur **Oui**. Le redémarrage peut prendre jusqu'à 30 minutes.

Configuration post-installation

Au cours de l'installation de vSphere Data Protection, lorsque vous exécutez l'utilitaire de configuration pour la première fois, il fonctionne en mode d'installation. Ce mode vous permet de définir les paramètres réseau, le fuseau horaire, le mot de passe de l'appliance et les informations d'identification vCenter. Après l'installation initiale, l'utilitaire VDP-configure s'exécute en mode de maintenance et affiche une autre interface utilisateur.

Pour accéder à VDP-Configure, ouvrez un navigateur Web et entrez :

https://*<adresse IP de l'appliance VDP>*:8543/vdp-configure/

L'interface de maintenance offre les fonctionnalités suivantes :

- Affichage de l'état des services : vous permet de voir les services actuellement actifs (ou actuellement arrêtés) sur l'appliance.
- Démarrage et arrêt de services : vous permet de démarrer et arrêter les services sélectionnés sur l'appliance.
- Collecte des logs : vous permet de télécharger les logs actuels de l'appliance.
- Affichage ou modification de la configuration de vSphere Data Protection : vous permet d'afficher ou de modifier les paramètres réseau, de configurer la gestion des licences vCenter ou d'afficher ou de modifier les paramètres système (fuseau horaire et informations d'identification vSphere Data Protection).
- Retour arrière d'une appliance : permet de restaurer une appliance à un état antérieur connu et valide (voir « Utilisation de points de contrôle et retour arrière » à la page 35).
- Mise à niveau : vous permet de mettre à niveau les images ISO sur l'appliance vSphere Data Protection.

Onglet État

Cet onglet permet d'afficher (et de démarrer ou d'arrêter) les services vSphere Data Protection.

Gestion des options d'état

L'écran gauche de l'onglet État présente l'état des services clés de l'appliance vSphere Data Protection. L'état des services suivants s'affiche :

Tableau 2-2. Description des services actifs sur l'appliance vSphere Data Protection

Service	Description
Services de base	Services qui concernent le moteur de sauvegarde de l'appliance. Si ces services sont désactivés, aucune procédure de sauvegarde (planifiée ou à la demande) ne peut s'exécuter et aucune activité de restauration ne peut être amorcée.
Services de gestion	Ces services ne doivent être arrêtés que sous la supervision du support technique.
Services de système de fichiers	Ces services permettent de monter des sauvegardes pour des opérations de restauration en mode fichier.
Services de restauration en mode fichier	Ces services permettent de prendre en charge la gestion d'opérations de restauration en mode fichier.
Services de maintenance	Ces services permettent d'effectuer des tâches de maintenance consistant, par exemple, à évaluer si des périodes de rétention de sauvegarde ont expiré. Ils sont désactivés les premières 24 à 48 heures de fonctionnement de l'appliance vSphere Data Protection. Ainsi, davantage de temps est alloué aux sauvegardes initiales.
Planificateur des sauvegardes	Le planificateur des sauvegardes est le service qui démarre les procédures de sauvegarde planifiées. S'il est arrêté, aucune sauvegarde n'est exécutée. Toutefois, vous pouvez lancer des sauvegardes à la demande.

L'état affiché pour ces services peut être :

- Démarrage en cours
- Échec du démarrage
- Exécution
- Arrêt en cours
- Échec de l'arrêt
- Arrêté
- État de chargement-obtention
- Irrécupérable (services de base uniquement)
- Restauration en cours (services de gestion uniquement)
- Échec de la restauration (services de gestion uniquement)

Démarrage et arrêt de services

Sur l'écran d'état, vous pouvez démarrer des services arrêtés en cliquant sur **Démarrer** ou arrêter des services actifs en cliquant sur **Arrêter**. En général, il convient cependant d'arrêter des services actifs sous la supervision du support technique.

Si vous voyez qu'un service est arrêté, vous pouvez essayer de le redémarrer en cliquant sur **Démarrer,** mais dans certains cas, d'autres étapes de dépannage sont nécessaires pour que le service fonctionne correctement.

Collecte des fichiers log

Le groupe de fichiers log est conçu pour faciliter l'envoi des logs de l'appliance vSphere Data Protection au personnel de support. Vous pouvez télécharger tous les logs à partir des services vSphere Data Protection sous la forme d'un groupe de logs en cliquant sur **Collecter les logs**. Une boîte de dialogue d'enregistrement s'ouvre pour vous permettre de télécharger le groupe de logs dans le système de fichiers de l'ordinateur sur lequel votre navigateur Web s'exécute. Le groupe de logs est nommé LogBungle.zip.

Onglet Configuration

Cet onglet permet d'afficher et de modifier la configuration de vSphere Data Protection.

La configuration de vSphere Data Protection qui peut être affichée ou modifiée comprend les paramètres suivants :

- Paramètres réseau
  - Adresse IP
  - Masque de réseau
  - Passerelle
  - DNS primaire
  - DNS secondaire
  - Nom d'hôte
  - Domaine
- Gestion des licences vCenter
  - Nom d'utilisateur vCenter
  - Mot de passe vCenter
  - Nom d'hôte vCenter
  - Port vCenter
  - Nom d'hôte SSO
  - Port SSO
- Paramètres système
  - Fuseau horaire
  - Informations d'identification VDP (changement de mot de passe VDP)

Onglet Retour arrière

L'onglet Retour arrière permet de revenir à un point de contrôle connu en cas de corruption des données de vSphere Data Protection.

REMARQUE L'utilisation du retour arrière est décrite dans « Utilisation de points de contrôle et retour arrière » à la page 35.

Onglet Mise à niveau

Cet onglet vous permet de mettre à niveau les images ISO sur l'appliance vSphere Data Protection.

REMARQUE La réalisation de mises à niveau est décrite dans « Utilisation de VDP Configure » à la page 20.

Utilisation de VDP Configure

L'utilitaire VDP Configure s'utilise lors de la configuration post-installation.

Conditions préalables

L'appliance vSphere Data Protection doit être installée et configurée. Vous devez ensuite vous connecter à l'aide du compte administrateur vSphere Data Protection.

Procédure

1 Ouvrez un navigateur Web et entrez :

https://*<adresse IP de l'appliance VDP>*:8543/vdp-configure/

2 Sur l'écran Connexion VMware, saisissez les informations suivantes :

a Utilisateur : **root**

b Mot de passe : ***mot de passe VDP***

c Cliquez sur **Connexion**.

3 (Facultatif) Pour afficher les services vSphere Data Protection, cliquez sur l'onglet **État**. Pour arrêter ou démarrer les services vSphere Data Protection, cliquez sur le bouton correspondant d'arrêt ou de démarrage.

4 (Facultatif, à la demande du support de VMware) Pour créer des fichiers log de support, cliquez sur l'onglet **État**, puis sur le bouton **Collecte des logs**. Enregistrez le fichier de groupe de logs et suivez les instructions du support VMware pour transmettre ce fichier.

5 (Facultatif) Pour afficher ou modifier la configuration de vSphere Data Protection, cliquez sur l'onglet **État**.

- Sous Paramètres Réseau, affichez ou modifiez la configuration. Si vous avez modifié la configuration, cliquez sur le bouton **Enregistrer**.
- Sous Gestion des licences vCenter, vous pouvez modifier les paramètres. Pour ce faire, cliquez sur l'icône du verrou. Si vous modifiez les paramètres de gestion des licences vCenter, les paramètres actuels des procédures de sauvegarde seront perdus, et vous devrez reconfigurer les procédures de sauvegarde. Si vous avez effectué des modifications, cliquez sur le bouton **Enregistrer**.
- Sous Paramètres système, vous pouvez afficher ou modifier le fuseau horaire. Si vous avez modifié le fuseau horaire, cliquez sur le bouton **Enregistrer**. Vous pouvez modifier le mot de passe vSphere Data Protection en cliquant sur le bouton **Modifier le mot de passe VDP**.

Mise à niveau de l'appliance VMware vSphere Data Protection

Le processus de mise à niveau comporte les étapes générales suivantes :

1 Création d'un snapshot de l'appliance vSphere Data Protection

2 Installation de la mise à niveau

3 Suppression du snapshot

REMARQUE Après la mise à niveau de l'appliance, lorsque vous vous connectez au vSphere Web Client pour la première fois, il n'affiche pas vSphere Data Protection en tant qu'option. Vous devez vous déconnecter de vSphere Web Client et vous reconnecter. Les connexions suivantes afficheront vSphere Data Protection en tant qu'option.

Conditions préalables

Pour effectuer une mise à niveau logicielle, vous devez télécharger une image ISO de la mise à niveau. En outre, tous les services vSphere Data Protection doivent être en cours d'exécution.

Création d'un snapshot de l'appliance vSphere Data Protection

Au moment de l'installation, les disques virtuels utilisés par l'appliance vSphere Data Protection sont définis sur le mode Indépendant - Persistant. Toutefois, pour pouvoir réaliser un snapshot, vous devez redéfinir temporairement les disques sur le mode Dépendant.

Pour créer un snapshot de l'appliance VMware vSphere Data Protection :

1 Connectez-vous à vCenter Server à l'aide du vSphere Web Client en tant qu'utilisateur autorisé à modifier les paramètres matériels et à réaliser des snapshots.

2 Cliquez sur **Hôtes et clusters**

3 Dans l'arborescence de gauche, cliquez sur les flèches de développement jusqu'à ce que l'appliance vSphere Data Protection s'affiche.

4 Cliquez avec le bouton droit de la souris sur l'appliance vSphere Data Protection et sélectionnez **Arrêt de l'OS invité**.

5 Cliquez sur **Oui**. Patientez jusqu'à l'arrêt de l'appliance vSphere Data Protection. Cette opération peut prendre quelques minutes.

6 Cliquez avec le bouton droit de la souris sur l'appliance vSphere Data Protection et sélectionnez **Modifier les paramètres**.

7 En commençant par le disque dur 2, cliquez sur la flèche de développement.

8 Dans le tableau Matériel virtuel, dans la ligne Mode Disque, cliquez sur **Dépendant**.

9 Poursuivez avec le disque dur 3 en répétant l'étape 8 jusqu'à ce que tous les disques restants soient définis sur le mode Dépendant.

10 Cliquez sur **OK**.

11 Cliquez avec le bouton droit de la souris sur l'appliance vSphere Data Protection et sélectionnez **Toutes les actions vCenter > Snapshot> Créer un snapshot**.

12 Saisissez le nom du snapshot. Entrez une description facultative. Cliquez sur **OK**.

13 Cliquez avec le bouton droit de la souris sur l'appliance vSphere Data Protection et sélectionnez **Mise sous tension**.

Installation de la mise à niveau

1 Connectez-vous au vCenter Server à l'aide du vSphere Web Client en tant qu'administrateur.

2 Cliquez sur **Hôtes et clusters**

3 Dans l'arborescence de gauche, cliquez sur les flèches de développement jusqu'à ce que l'appliance vSphere Data Protection s'affiche.

4 Cliquez avec le bouton droit de la souris sur l'appliance vSphere Data Protection et sélectionnez **Modifier les paramètres**.

5 Sous l'onglet Matériel virtuel, développez le lecteur CD/DVD. Dans le menu déroulant, sélectionnez **Fichier ISO du datastore**.

6 Sous Sélectionner un fichier, accédez à l'image ISO et sélectionnez-la. Cliquez sur **OK**.

7 À droite de l'image ISO du datastore, sélectionnez **Connecté**. Cliquez sur **OK**. En fonction de la taille du fichier ISO, l'opération de montage peut prendre quelques minutes.

8 Ouvrez un navigateur Web et entrez :

https://<*adresse IP de l'appliance VDP*>:8543/vdp-configure/

9 Sur l'écran Connexion VMware, saisissez les informations suivantes :

   a Utilisateur : **root**

   b Mot de passe : ***mot de passe VDP***

   c Cliquez sur **Connexion**.

10 Cliquez sur l'onglet **Mise à niveau**. Vérifiez que l'image ISO est disponible et que son état est Prêt. Dans le cas contraire, il se peut qu'elle soit encore en cours de chargement.

REMARQUE Si l'image ISO n'apparaît pas, déconnectez-vous de VDP-Configure et reconnectez-vous.

11 Cliquez sur **Mise à niveau de la VDP**. L'installation de la mise à niveau commence. Cette partie de l'installation de la mise à niveau peut prendre un certain temps, mais la barre d'état indiquera la progression de l'opération.

12 Une fois la mise à niveau installée sans erreur, cliquez sur **OK**. Cliquez avec le bouton droit de la souris sur l'appliance vSphere Data Protection et sélectionnez **Arrêt de l'OS invité**.

Suppression du snapshot

Il est vivement conseillé de supprimer les snapshots une fois la mise à niveau réussie.

Pour supprimer le snapshot :

1 Connectez-vous au vCenter Server à l'aide du vSphere Web Client en tant qu'utilisateur autorisé à modifier les paramètres matériels et à supprimer des snapshots.

2 Cliquez sur **Hôtes et clusters**

3 Dans l'arborescence de gauche, cliquez sur les flèches de développement jusqu'à ce que l'appliance vSphere Data Protection s'affiche.

4 Cliquez avec le bouton droit de la souris sur l'appliance vSphere Data Protection et sélectionnez **Toutes les actions vCenter > Snapshot> < Snapshot Manager**.

5 Cliquez sur le snapshot que vous avez créé pour l'appliance vSphere Data Protection.

6 Cliquez sur **Supprimer**, puis sur **Oui**.

7 Cliquez sur **Fermer**.

8 Cliquez avec le bouton droit de la souris sur l'appliance vSphere Data Protection et sélectionnez **Modifier les paramètres**.

9 En commençant par le disque dur 2, cliquez sur la flèche de développement.

10 Dans le tableau Matériel virtuel, dans la ligne Mode Disque, cliquez sur **Indépendant - Persistant**.

11 Poursuivez avec le disque dur 3 en répétant l'étape 10 jusqu'à ce que tous les disques restants soient définis sur le mode Indépendant - Persistant.

12 Démontez l'image ISO. Sous l'onglet Matériel virtuel, développez le lecteur CD/DVD. Dans le menu déroulant, sélectionnez Périphérique client. Cliquez sur **OK**.

13 Cliquez sur **OK**.

14 Cliquez avec le bouton droit de la souris sur l'appliance vSphere Data Protection et sélectionnez **Mise sous tension**.

15 Une fois le redémarrage terminé, cliquez avec le bouton droit de la souris sur l'appliance vSphere Data Protection et sélectionnez **Modifier les paramètres**.

La mise à niveau de l'appliance vSphere Data Protection est terminée.

Utilisation de vSphere Data Protection 3

Une fois que l'application vSphere Data Protection (VDP) est installée et configurée, il est possible de la gérer via le vSphere Web Client for vSphere Data Protection.

Ce chapitre comporte les rubriques suivantes :

Comprendre l'interface utilisateur de vSphere Data Protection

Le vSphere Web Client for vSphere Data Protection fournit un certain nombre de nouveaux éléments d'interface utilisateur qui servent à configurer et à gérer vSphere Data Protection.

L'interface utilisateur de vSphere Data Protection comporte cinq onglets :

- **Mise en oeuvre** : vue d'ensemble des fonctionnalités de vSphere Data Protection et liens rapides vers l'assistant de création de procédure de sauvegarde et vers l'assistant de restauration.
- **Sauvegarde** : liste des procédures de sauvegarde planifiées et informations sur chacune d'elles. Vous pouvez également créer et modifier les procédures de sauvegarde à partir de cette page. Elle permet aussi d'exécuter une procédure de sauvegarde immédiatement.
- **Restauration** : liste des sauvegardes réussies que vous pouvez restaurer.
- **Rapports** : rapports d'état des sauvegardes sur les machines virtuelles dans vCenter.
- **Configuration** : affiche des informations sur les paramètres de configuration de vSphere Data Protection et permet de modifier certains de ces paramètres.

Chacun de ces onglets est décrit dans les rubriques qui suivent.

Onglet Mise en oeuvre

L'onglet Mise en oeuvre présente succinctement vSphere Data Protection et explique comment effectuer des tâches de configuration courantes.

Tableau 3-1. onglet Mise en oeuvre

Icône	Nom	Description
	Créer une procédure de sauvegarde	Démarre l'assistant Procédure de sauvegarde. Pour plus d'informations, reportez-vous à la rubrique « Utiliser l'assistant Procédure de sauvegarde » à la page 28.
	Restaurer une VM	Démarre l'assistant Restaurer une machine virtuelle. Pour plus d'informations, reportez-vous à la rubrique « Restauration de machines virtuelles à partir de la sauvegarde » à la page 30.
	Voir une présentation	Permet de basculer de l'affichage actuel vers l'onglet Rapports qui permet de vérifier l'état des procédures existantes. Pour plus d'informations, reportez-vous à la rubrique « Affichage de rapports » à la page 30.

Onglet Sauvegarde

L'onglet Sauvegarde affiche des informations sur les procédures de sauvegarde et leur état. Il permet également de créer, modifier, supprimer, activer/désactiver et exécuter des procédures de sauvegarde immédiates.

Tableau 3-2. Icônes de l'onglet Sauvegarde

Icône	Nom	Description
	Nouveau	Démarre l'assistant Procédure de sauvegarde. Pour plus d'informations, reportez-vous à la rubrique « Utiliser l'assistant Procédure de sauvegarde » à la page 28.
	Modifier	Démarre l'assistant Procédure de sauvegarde pour modifier une procédure.
	Supprimer	Supprime la procédure de sauvegarde sélectionnée.
	Activer/Désactiver	Active ou désactive la procédure de sauvegarde.
	Sauvegarder maintenant	Démarre une sauvegarde immédiate.

L'onglet Sauvegarde affiche une liste des procédures de sauvegarde créées. Les procédures de sauvegarde sont répertoriées dans un tableau contenant les informations suivantes :

Tableau 3-3. Description des colonnes de l'onglet Sauvegarde

Colonne	Description
Nom	Nom de la procédure de sauvegarde.
État	Activé ou désactivé. Les procédures de sauvegarde désactivées ne sont pas exécutées.
Dernière heure de début	Dernier moment auquel la procédure de sauvegarde a été démarrée.
Durée	Durée de la dernière procédure de sauvegarde.
Prochaine heure d'exécution	Heure de la prochaine exécution planifiée.
Nombre de réussites	Nombre de VM sauvegardées sans erreur la dernière fois que la procédure de sauvegarde a été exécutée.
Nombre d'échecs	Nombre de VM non sauvegardées la dernière fois que la procédure de sauvegarde a été exécutée.

Onglet Restauration

L'onglet Restauration affiche une liste des VM qui ont été sauvegardées sur l'appliance vSphere Data Protection. En parcourant la liste des sauvegardes, vous pouvez sélectionner et restaurer des sauvegardes spécifiques. Au fil du temps, les informations affichées sous l'onglet Restauration peuvent ne plus être à jour. Pour voir les informations les plus récentes sur les sauvegardes disponibles en vue d'une restauration, cliquez sur **Actualiser**.

Les icônes suivantes sont utilisées sous l'onglet Restauration.

Tableau 3-4. Icônes de l'onglet Restauration

Icône	Nom	Description
	Restauration	Démarre la restauration de machines virtuelles à partir de la sauvegarde, ce qui permet de configurer la façon dont les machines virtuelles sont restaurées à l'état enregistré dans les points de restauration sélectionnés. Pour plus d'informations, reportez-vous à la rubrique « Restauration de machines virtuelles à partir de la sauvegarde » à la page 30. Par défaut, vSphere Data Protection gère le stockage et l'éventuelle suppression des points de restauration anciens selon la règle de rétention définie dans la procédure de sauvegarde.
	Verrouiller/Déverrouiller	Verrouille le point d'expiration d'une procédure de sauvegarde sur une date « sans fin ».
	Supprimer	Supprime les points de restauration sélectionnés.
	Effacer toutes les sélections	Efface toutes les sélections de l'onglet Restauration.

Onglet Rapports

Cet onglet présente succinctement l'appliance vSphere Data Protection et les VM du Virtual Center.

Onglet Configuration

Cet onglet vous permet de gérer les tâches de maintenance pour l'appliance vSphere Data Protection.

Vous pouvez effectuer trois tâches à partir de cet onglet :

- Afficher ou modifier la fenêtre de sauvegarde (voir « Configuration de la fenêtre de sauvegarde » à la page 32)
- Exécuter un contrôle d'intégrité (voir « Effectuer un contrôle d'intégrité manuel » à la page 34)
- Configurer les e-mails (voir « Configuration de la notification par e-mail » à la page 34)

Accès à vSphere Data Protection

vSphere Data Protection est accessible via le vSphere Web Client.

REMARQUE La gestion de vSphere Data Protection s'effectue uniquement via le vSphere Web Client. Le vSphere Client ne permet pas la gestion de vSphere Data Protection.

Conditions préalables

Avant d'utiliser vSphere Data Protection, vous devez installer et configurer l'appliance vSphere Data Protection comme décrit dans la rubrique « Installation et configuration de vSphere Data Protection » à la page 11.

Procédure

1 Accédez à vSphere Web Client à l'aide d'un navigateur Web.

https://<*adresse IP_vCenter_Server*>:9443/vsphere-client/

2 À la page des informations d'identification, entrez un nom d'utilisateur et un mot de passe vCenter, puis cliquez sur **Connexion**.

vSphere Data Protection utilise ces informations pour se connecter à vCenter afin d'effectuer des sauvegardes ; le compte utilisateur indiqué doit donc disposer de droits d'administration.

3 Dans le vSphere Web Client, sélectionnez **vSphere Data Protection**.

4 À la page d'accueil de vSphere Data Protection, sélectionnez l'appliance vSphere Data Protection et cliquez sur **Connecter**.

Changement d'appliance vSphere Data Protection

Chaque vCenter Server peut prendre en charge jusqu'à 10 appliances vSphere Data Protection. Vous pouvez changer d'appliance en la choisissant dans la liste déroulante située à droite du libellé Changer d'appliance.

REMARQUE Les appliances vSphere Data Protection figurant dans la liste sont triées dans l'ordre alphabétique. Le premier élément affiché ne correspond donc pas forcément à l'appliance active. Sur l'écran vSphere Data Protection, le nom de l'appliance figurant à gauche correspond à l'appliance active, et celui visible dans la liste déroulante correspond à la première appliance dans la liste des appliances disponibles.

Créer des procédures de sauvegarde

Vous pouvez créer des procédures de sauvegarde identifiant les machines virtuelles à sauvegarder, la fréquence des sauvegardes et la période de rétention pour le stockage des sauvegardes. vSphere Data Protection utilise une fenêtre de sauvegarde pour créer des sauvegardes et la règle de rétention ou pour supprimer d'anciennes sauvegardes particulières.

Machines virtuelles

Vous pouvez définir des collections de VM, par exemple toutes celles d'un datacenter, ou sélectionner des VM spécifiques. Si vous sélectionnez tout un pool de ressources, datacenter ou dossier, toutes les nouvelles VM qu'il contient sont incluses dans les sauvegardes suivantes. Si vous sélectionnez une VM, tous les disques qui y sont ajoutés sont inclus dans la sauvegarde. Si vous déplacez une VM du conteneur sélectionné vers un conteneur non sélectionné, elle est exclue de la sauvegarde.

Vous pouvez sélectionner manuellement une VM à sauvegarder pour vous assurer qu'elle est bien sauvegardée même en cas de déplacement.

REMARQUE L'utilisation de vSphere Data Protection pour sauvegarder une appliance vSphere Data Protection n'est pas prise en charge.

Calendrier

Le calendrier détermine la fréquence des sauvegardes de vos sélections. Les sauvegardes commenceront au début de la fenêtre de sauvegarde, le plus tôt possible. Vous pouvez planifier vos sauvegardes de sorte à les exécuter tous les jours, toutes les semaines ou à une date particulière dans le mois.

Règle de rétention

Les règles de rétention de sauvegarde vous permettent de définir la période de rétention d'une sauvegarde dans le système.

Une règle de rétention est attribuée à chaque sauvegarde lorsque cette dernière a lieu. Lorsque la rétention d'une sauvegarde expire, la sauvegarde est supprimée.

Le Tableau 3-5 décrit les règles de rétention pour les sauvegardes.

Tableau 3-5. Paramètres de règle de rétention

Paramètre de rétention	Description
Toujours	Permet de conserver les sauvegardes indéfiniment. Ce paramètre sert à s'assurer que toutes les sauvegardes auxquelles est attribuée cette règle de rétention sont conservées tout au long de la durée de vie du système.
Pour (période de rétention)	Permet de définir une période de rétention fixe en jours, semaines, mois ou années suivant la réalisation de la sauvegarde. Par exemple, vous pouvez indiquer que les sauvegardes doivent expirer après 6 mois.
Jusqu'à (date de fin)	Permet d'attribuer une date calendaire comme date d'expiration. Par exemple, vous pouvez indiquer que les sauvegardes expirent le 31 décembre 2013.
Pour (ce calendrier)	Permet de définir une période de rétention fixe sur une base quotidienne, hebdomadaire, mensuelle ou annuelle. Par exemple, vous pouvez indiquer que les sauvegardes doivent être conservées pendant 30 jours, chaque semaine pendant 52 semaines, chaque mois pendant 12 mois ou chaque année pendant 2 ans.

Prêt à terminer

Vérifiez les paramètres de la procédure de sauvegarde. Cette page comprend entre autres les informations suivantes :

- Nom de la procédure de sauvegarde
- Machines virtuelles qui seront sauvegardées par cette procédure
- Calendrier selon lequel les machines virtuelles seront sauvegardées
- Règle de rétention sélectionnée pour la sauvegarde

Utiliser l'assistant Procédure de sauvegarde

Utilisez l'assistant Procédure de sauvegarde pour définir les machines virtuelles qui doivent être sauvegardées et le moment auquel elles doivent l'être.

Procédure

1. Dans le vSphere Web Client, sélectionnez **vSphere Data Protection**.
2. À la page d'accueil de vSphere Data Protection, sélectionnez l'appliance vSphere Data Protection et cliquez sur **Connecter**.
3. Cliquez sur l'onglet **Sauvegarde**, puis sur **Nouveau** pour démarrer l'assistant Procédure de sauvegarde.
4. À la page Machines virtuelles, sélectionnez des VM ou des conteneurs de machines virtuelles à sauvegarder, puis cliquez sur **Suivant**.
5. À la page Calendrier, sélectionnez le calendrier de sauvegarde pour la procédure en question, puis cliquez sur **Suivant**.
6. À la page Règle de rétention, acceptez la règle par défaut ou définissez une autre règle, puis cliquez sur **Suivant**.
7. À la page Nom, entrez le nom de la procédure de sauvegarde, puis cliquez sur **Suivant**.
8. À la page Prêt à terminer, examinez les informations récapitulatives de la procédure de sauvegarde, puis cliquez sur **Terminer.**
9. Une fenêtre de confirmation vous indique que la procédure de sauvegarde a été créée sans erreur. Cliquez sur **OK**.

Sauvegarder maintenant

Une fois la procédure de sauvegarde créée, vous pouvez la démarrer manuellement en cliquant sur l'icône Sauvegarder maintenant.

Conditions préalables

Pour pouvoir utiliser l'option Sauvegarder maintenant, vous devez avoir installé et configuré vSphere Data Protection et avoir créé au moins une procédure de sauvegarde.

Procédure

1 Dans le vSphere Web Client, sélectionnez **vSphere Data Protection**.

2 À la page d'accueil de vSphere Data Protection, sélectionnez l'appliance vSphere Data Protection et cliquez sur **Connecter**.

3 Cliquez sur l'onglet **Sauvegarde** et sélectionnez une procédure de sauvegarde. Cliquez sur **Sauvegarder maintenant** et sélectionnez Sauvegarder toutes les sources ou Sauvegarder uniquement les sources périmées.

- L'option Sauvegarder toutes les sources permet de sauvegarder toutes les procédures.
- L'option Sauvegarder uniquement les sources périmées permet de sauvegarder les procédures de sauvegarde qui ont échoué au cours de la dernière tentative de sauvegarde.

Restauration de machines virtuelles

Vous pouvez définir les machines virtuelles que vous souhaitez restaurer, leur mode et leur emplacement de restauration à l'aide de l'assistant Restaurer une machine virtuelle.

ATTENTION Si la VM que vous essayez de restaurer contient un snapshot, l'opération échoue. Supprimez les snapshots de la VM avant de démarrer la restauration.

Sélectionner une sauvegarde

Cette option permet de définir les machines virtuelles à restaurer. Les restaurations sont similaires à la création de procédures de sauvegarde en ce sens que vous pouvez définir un conteneur de VM ou des machines virtuelles spécifiques. Il est possible de restaurer des machines virtuelles à d'autres emplacements.

Définir les options de restauration

Cette option permet d'indiquer l'emplacement où la sauvegarde sera restaurée.

Vous pouvez indiquer :

- si la sauvegarde sera restaurée à l'emplacement d'origine
- si la sauvegarde sera restaurée à un autre emplacement
  - Nouveau nom
  - Destination
  - Emplacement du datastore

Pour cloner une machine virtuelle, renommez celle que vous restaurez.

Prêt à terminer

Vérifiez les paramètres de la procédure de restauration. Le résumé contient : des informations sur le nombre de VM qui seront restaurées et qui seront créées.

Restauration de machines virtuelles à partir de la sauvegarde

Vous pouvez restaurer des machines virtuelles à un état précédent à l'aide de l'assistant de restauration de machines virtuelles.

Conditions préalables

Pour pouvoir restaurer des machines virtuelles, vous devez avoir configuré vSphere Data Protection et avoir créé au moins une sauvegarde à partir de laquelle effectuer la restauration.

Procédure

1 Dans le vSphere Web Client, sélectionnez **vSphere Data Protection**.

2 À la page d'accueil de vSphere Data Protection, sélectionnez l'appliance vSphere Data Protection et cliquez sur **Connecter**.

3 Cliquez sur l'onglet **Restauration** et sur le bouton **Restaurer**.

4 L'assistant de restauration de machines virtuelles s'ouvre.

5 À la page Sélectionner une sauvegarde, indiquez une source à partir de laquelle restaurer les machines virtuelles, puis cliquez sur **Suivant**.

6 Si la VM comporte plusieurs points de restauration, désélectionnez tous les points qui ne seront pas restaurés. Seul un point de sauvegarde doit être sélectionné.

7 À la page Définir les options de restauration, vérifiez que le point de restauration du client et de la sauvegarde est correct. Sélectionnez Restaurer à l'emplacement d'origine ou, pour effectuer la restauration à un autre emplacement, désélectionnez la case Restaurer à l'emplacement d'origine et indiquez une autre destination et un autre datastore. Cliquez sur **Suivant**.

8 À la page Prêt à terminer, examinez la configuration et cliquez sur **Termin**er.

Les machines virtuelles sont restaurées comme indiqué dans l'assistant.

Affichage de la progression de la procédure de restauration

Une fois qu'une procédure de restauration est démarrée, vous pouvez afficher le processus de restauration en cours dans le volet Tâche récente.

Verrouillage d'une procédure de sauvegarde

L'icône du verrou permet de redéfinir le point d'expiration d'une procédure de sauvegarde sur une date « sans fin ». Cela empêche l'expiration manuelle d'une procédure de sauvegarde et sa suppression automatique après la date d'expiration. L'option de verrouillage n'empêche pas la suppression d'une procédure de sauvegarde : un administrateur peut supprimer manuellement une procédure verrouillée. Pour verrouiller une procédure de sauvegarde, sélectionnez-la sous l'onglet Restauration, puis cliquez sur l'icône du verrou. Les procédures de sauvegarde verrouillées sont signalées par la présence d'un verrou jaune à gauche de leur nom.

Affichage de rapports

L'onglet Rapports présente l'état actuel des éléments suivants :

- État de l'appliance
- Capacité utilisée
- État du contrôle d'intégrité
- Sauvegardes récentes réussies
- Sauvegardes récentes en échec

Filtrage de l'onglet Rapports

Par défaut, l'onglet Rapports affiche toutes les machines virtuelles associées au vCenter Server. L'option Filtrer de l'onglet Rapports permet de filtrer par :

- Afficher tout
- VM
  - Nom
  - État
  - Dernière sauvegarde réussie
- Dernière procédure de sauvegarde
  - Nom
  - État
  - Date

Gestion de la configuration

L'onglet Configuration permet d'afficher et de modifier les informations de configuration. Les sujets suivants sont traités dans cette rubrique :

- « Afficher et modifier les détails d'une appliance de sauvegarde » à la page 32
- « Configuration de la fenêtre de sauvegarde » à la page 32
- « Modifier les paramètres de la fenêtre de maintenance » à la page 34
- « Effectuer un contrôle d'intégrité manuel » à la page 34
- « Configuration de la notification par e-mail » à la page 34

Vous pouvez afficher les détails d'une appliance de sauvegarde, la présentation du stockage et la configuration de la fenêtre de sauvegarde sous l'onglet Configuration.

Afficher et modifier les détails d'une appliance de sauvegarde

Les détails d'une appliance de sauvegarde comprennent les informations suivantes :

- Adresse IP
- Version de l'appliance vSphere Data Protection
- État
- vCenter Server
- Utilisateur actuel
- Heure locale
- Fuseau horaire
- Espace disponible
- Taille avec déduplication
- Taille sans déduplication

REMARQUE La capacité de stockage est affichée en GiO (et non pas en Go), qui correspond à 1 024 Mo.

Configuration de la fenêtre de sauvegarde

Chaque journée de 24 heures est divisée en trois fenêtres opérationnelles : la fenêtre de sauvegarde, la fenêtre réservée et la fenêtre de maintenance au cours desquelles diverses activités système se déroulent.

Fenêtre de sauvegarde

La fenêtre de sauvegarde est l'intervalle de temps réservé aux sauvegardes planifiées normales au cours de la journée.

- Incidence opérationnelle : par défaut, aucune activité de maintenance n'a lieu au cours de la fenêtre de sauvegarde.
- Paramètres par défaut : la fenêtre de sauvegarde par défaut débute à 20h00, heure du serveur local, et se poursuit sans interruption pendant 12 heures jusqu'à 8h00 le lendemain.
- Personnalisation : vous pouvez personnaliser l'heure de début de la fenêtre de sauvegarde et sa durée afin de répondre aux exigences spécifiques du site.

vSphere Data Protection tente de sauvegarder chaque machine virtuelle d'une procédure une fois par jour au cours de sa fenêtre de sauvegarde. Les sauvegardes débutent au début de la fenêtre de sauvegarde, et jusqu'à huit procédures de sauvegarde au maximum peuvent être exécutées simultanément.

REMARQUE Si plusieurs appliances vSphere Data Protection sauvegardent les mêmes machines virtuelles, les fenêtres de sauvegarde doivent être ajustées de sorte que les procédures de sauvegarde de différentes appliances ne se chevauchent pas. Si tel est le cas, les sauvegardes échouent.

Fenêtre réservée

La fenêtre réservée est l'intervalle de temps, au cours de la journée, réservé aux activités de maintenance des serveurs, telles que la récupération d'espace disque, qui nécessitent un accès non restreint au serveur. La récupération d'espace disque supprime les segments de données orphelins qui ne sont plus référencés dans des sauvegardes stockées sur le système.

- Incidence opérationnelle : aucune activité de sauvegarde ou d'administration n'a lieu au cours de la fenêtre réservée. Vous pouvez effectuer des restaurations.
- Paramètres par défaut : la fenêtre réservée par défaut débute à 08h00, heure du serveur local, et se poursuit sans interruption pendant trois heures jusqu'à 11h00 le lendemain.
- Personnalisation : vous pouvez personnaliser la durée de la fenêtre réservée afin de répondre aux exigences spécifiques du site.

Toute modification de la durée de la fenêtre réservée a une incidence sur celle de la fenêtre de maintenance. Par exemple, si vous réduisez la durée de la fenêtre réservée de 3 à 2 heures, vous augmentez la durée de la fenêtre de maintenance d'une heure puisqu'elle commence une heure plus tôt. Il n'y a pas d'incidence sur la fenêtre de sauvegarde.

Fenêtre de maintenance

La fenêtre de maintenance est l'intervalle de temps, au cours de la journée, réservé à des activités régulières de maintenance des serveurs, telles que la validation du contrôle d'intégrité.

- Incidence opérationnelle : il arrive que les activités de sauvegarde ou d'administration ne soient pas autorisées sur de brèves périodes.

  Il est possible de démarrer des sauvegardes au cours de la fenêtre de maintenance, mais non sans incidence sur les activités de sauvegarde et de maintenance. Pour cette raison, réduisez au minimum les activités de sauvegarde ou d'administration au cours de la fenêtre de maintenance. Vous pouvez cependant effectuer des restaurations.

  Le contrôle d'intégrité et les sauvegardes peuvent se chevaucher, mais cela peut entraîner un conflit d'accès des ressources d'E/S susceptible d'allonger la durée de ces deux activités, voire de provoquer leur échec.

- Paramètres par défaut : la fenêtre de maintenance par défaut débute à 11h00, heure du serveur local, et se poursuit sans interruption pendant neuf heures jusqu'à 20h00 le même soir.

- Personnalisation : bien que la fenêtre de maintenance ne puisse pas être directement personnalisée, son heure de début et sa durée sont dérivées des paramètres de la fenêtre réservée et de sauvegarde.

La fenêtre de maintenance débute immédiatement après la fenêtre réservée et se poursuit jusqu'à l'heure de début de la fenêtre de sauvegarde.

Contrôle d'intégrité

Cette opération permet de vérifier et de maintenir l'intégrité des données sur la zone de stockage de déduplication. La solution vSphere Data Protection est conçue pour réaliser des contrôles d'intégrité incrémentiels ou complets au cours de la fenêtre de maintenance. Les contrôles d'intégrité incrémentiels vérifient l'intégrité des points de contrôle qui ont été ajoutés à la zone de stockage de déduplication depuis le contrôle d'intégrité complet ou incrémentiel le plus récent. La solution vSphere Data Protection est également conçue pour effectuer un contrôle d'intégrité de tous les points de contrôle une fois par jour. Pour plus d'informations, reportez-vous à la rubrique « Utilisation de points de contrôle et retour arrière » à la page 35.

La fenêtre de maintenance doit être utilisée pour éviter les situations où les contrôles d'intégrité peuvent consommer des ressources informatiques ou autrement interférer avec les opérations de sauvegarde en cours. Par conséquent, la fenêtre de maintenance et la fenêtre de sauvegarde sont définies de telle manière qu'elles ne se chevauchent pas. La maintenance est arrêtée si elle ne se termine pas dans la fenêtre définie. Même si la maintenance est arrêtée, la destination n'est pas verrouillée pour d'autres opérations telles qu'une sauvegarde ou une restauration. La prochaine fois que la fenêtre de maintenance de destination s'ouvrira, l'opération reprendra là où elle s'est arrêtée. Pour plus d'informations sur la configuration de la fenêtre de maintenance, reportez-vous à la rubrique « Modifier les paramètres de la fenêtre de maintenance » à la page 34.

En outre, le contrôle d'intégrité peut être démarré manuellement. Dans ce cas, il effectue toujours un contrôle complet de la destination dans son intégralité sans utiliser la fenêtre de maintenance. En principe, les opérations de sauvegarde et de restauration sont autorisées depuis la zone de stockage de déduplication alors même qu'un contrôle d'intégrité est en cours. Si un point de restauration est sélectionné manuellement pour suppression, les sauvegardes ne sont pas autorisées au cours du contrôle d'intégrité, mais les opérations de restauration le sont. Si des points de restauration endommagés sont détectés dans la zone de stockage de déduplication au cours d'un contrôle d'intégrité, un contrôle manuel doit être effectué après leur sélection pour les supprimer. Les sauvegardes et restaurations ne sont pas autorisées au cours de ce contrôle d'intégrité exécuté manuellement. Pour plus d'informations sur le démarrage manuel d'un contrôle d'intégrité, reportez-vous à la rubrique « Effectuer un contrôle d'intégrité manuel » à la page 34.

vSphere Data Protection stocke les informations sur la progression d'un contrôle d'intégrité. Par conséquent, si l'appliance vSphere Data Protection arrête le contrôle d'intégrité, le processus peut être redémarré à partir de l'endroit où il a été arrêté. Ainsi, ce qui a déjà été accompli par le contrôle d'intégrité n'est pas perdu. L'appliance arrête les contrôles d'intégrité lorsque la fenêtre de maintenance est dépassée. Le suivi de la progression permet de s'assurer que les contrôles d'intégrité sont menés jusqu'au bout. Les contrôles d'intégrité arrêtés manuellement par un utilisateur n'enregistrent pas leurs informations de progression. Par conséquent, ils recommencent depuis le début après un arrêt de ce type.

Modifier les paramètres de la fenêtre de maintenance

Modifiez les paramètres de la fenêtre de maintenance sous l'onglet Configuration.

Conditions préalables

Pour pouvoir modifier les paramètres de la fenêtre de maintenance, vous devez installer et configurer vSphere Data Protection.

Procédure

1 Dans le vSphere Web Client, sélectionnez **vSphere Data Protection**.

2 À la page d'accueil de vSphere Data Protection, sélectionnez l'appliance vSphere Data Protection et cliquez sur **Connecter**.

3 Cliquez sur l'**onglet Configuration**.

4 Dans Configuration de la fenêtre de sauvegarde, cliquez sur **Modifier**.

5 Sélectionnez l'heure de début et la durée de la sauvegarde, ainsi que la durée de la fenêtre réservée, puis cliquez sur **Enregistrer**.

Effectuer un contrôle d'intégrité manuel

Vous pouvez effectuer manuellement des contrôles d'intégrité sous l'onglet Configuration.

Conditions préalables

Pour pouvoir exécuter un contrôle d'intégrité, vous devez configurer vSphere Data Protection.

Procédure

1 Dans le vSphere Web Client, sélectionnez **vSphere Data Protection**.

2 À la page d'accueil de vSphere Data Protection, sélectionnez l'appliance vSphere Data Protection et cliquez sur **Connecter**.

3 Cliquez sur l'**onglet Configuration**.

4 Dans Configuration de la fenêtre de sauvegarde, cliquez sur l'icône des paramètres (en haut à droite de l'onglet Configuration), puis cliquez sur **Exécuter le contrôle d'intégrité**.

5 Une fenêtre de confirmation s'ouvre. Cliquez sur **Oui**.

Configuration de la notification par e-mail

Si la notification par e-mail est activée, des e-mails contenant les informations suivantes sont envoyés :

- État de l'appliance vSphere Data Protection
- Résumé des procédures de sauvegarde
- Résumé des machines virtuelles

Conditions préalables

L'envoi de rapports par e-mail ne peut être configuré que si le compte e-mail existe.

Procédure

1 Dans le vSphere Web Client, sélectionnez **vSphere Data Protection**.

2 À la page d'accueil de vSphere Data Protection, sélectionnez l'appliance vSphere Data Protection et cliquez sur **Connecter**.

3 Cliquez sur l'**onglet Configuration**.

4 Cliquez sur le bouton **E-mail**.

5 Cliquez sur le bouton **Modifier** dans l'angle inférieur droit de l'écran.

6 Indiquez les éléments suivants :

   a Sélectionnez **Activer l'envoi des rapports par e-mail**.

   b Définissez le **serveur de messagerie sortant**.

   c (facultatif) Sélectionnez **Mon serveur requiert une authentification.** Si cette option est sélectionnée, indiquez le **Nom d'utilisateur** et le **Mot de passe** associés.

   d Définissez l'**adresse de l'expéditeur**.

   e Définissez la ou les **adresses de destination**.

   f Sélectionnez le ou les **jours de l'envoi**.

   g Sélectionnez le **paramètre régional du rapport**.

7 Cliquez sur le bouton **Enregistrer**.

Utilisation de points de contrôle et retour arrière

Un point de contrôle est une sauvegarde de système entier effectuée à la seule fin de faciliter la reprise après sinistre. Les points de contrôle sont programmés et créés une fois par jour au cours de la fenêtre de maintenance (voir « Fenêtre de maintenance » à la page 33). vSphere Data Protection stocke deux points de contrôle (un validé et un non validé). Le retour arrière permet de restaurer l'appliance vSphere Data Protection à un état connu de bon fonctionnement à l'aide des données stockées dans un point de contrôle validé. Par défaut, les services de maintenance sont désactivés pour les 24 à 48 heures qui suivent le déploiement d'une appliance. Cela permet de disposer d'une fenêtre de sauvegarde plus longue pour faciliter les sauvegardes initiales.

Dans le cas d'un arrêt non planifié, l'appliance retourne en arrière au dernier point de contrôle validé dès qu'elle est redémarrée. Ce comportement est normal et permet d'éviter la détérioration de l'appliance.

Lorsque l'appliance est déployée, un point de contrôle immédiat est créé. Il contient les paramètres de l'appliance enregistrés avec l'installation. Si un arrêt non planifié a lieu au cours des premières 24 à 48 heures du déploiement, l'appliance retourne en arrière au point de contrôle immédiat. Les procédures de sauvegarde ou les sauvegardes qui ont été créées entre la création du point de contrôle immédiat et l'arrêt non planifié seront perdues. Pour créer un point de contrôle au cours de cette période, exécutez manuellement un contrôle d'intégrité. Pour plus d'informations, reportez-vous à la rubrique « Effectuer un contrôle d'intégrité manuel » à la page 34.

REMARQUE Si vous utilisez le retour arrière, toutes les sauvegardes qui ont lieu après le point de contrôle sélectionné sont perdues.

Conditions préalables

Pour pouvoir exécuter un retour arrière, vous devez avoir installé et configuré vSphere Data Protection, et les points de contrôle doivent avoir été créés et validés.

ATTENTION Il est vivement conseillé d'effectuer un retour arrière uniquement jusqu'au point de contrôle validé le plus récent.

Procédure

1 Ouvrez un navigateur Web et entrez :

http://<*adresse IP de l'appliance VDP*>:8543/vdp-configure/

2 Dans l'écran Connexion VMware, saisissez les informations suivantes :

a Utilisateur : **root**

b Mot de passe : ***mot de passe VDP***

c Cliquez sur **Connexion**.

3 Cliquez sur l'onglet **Retour arrière**.

4 Cliquez sur **Déverrouiller pour activer le retour arrière de la VDP.**

5 Une boîte de dialogue d'avertissement vous avertit que toutes les sauvegardes qui auront lieu après le point de contrôle sélectionné seront perdues. Si cette solution est acceptable, entrez le mot de passe vSphere Data Protection et cliquez sur **OK**.

6 Sélectionnez un point de contrôle validé (valide=true) et cliquez sur **Effectuer le retour arrière de la VDP au point de contrôle sélectionné**.

Utilisation de la restauration en mode fichier

vSphere Data Protection crée des sauvegardes de machines virtuelles entières. Ces sauvegardes peuvent être restaurées dans leur intégralité à l'aide du vSphere Web Client for vSphere Data Protection. Toutefois, pour restaurer des fichiers particuliers à partir de ces machines virtuelles, utilisez le vSphere Data Protection Restore Client.

Le Restore Client vous permet de monter des sauvegardes de machine virtuelle spécifiques en tant que systèmes de fichiers et de parcourir le système pour rechercher les fichiers que vous souhaitez restaurer.

Le Restore Client fonctionne en deux modes :

- Connexion de base : permet de monter uniquement les sauvegardes créées à partir de la machine avec laquelle vous vous êtes connecté ; les fichiers seront restaurés sur ce client.

  Par exemple, si vous vous connectez au Restore Client en mode de connexion de base depuis un hôte Windows nommé WS44, vous serez en mesure de monter et de parcourir les sauvegardes de WS44 uniquement.

- Connexion avancée : permet de monter et de parcourir toutes les sauvegardes contenues dans vSphere Data Protection.

Seules huit sauvegardes au maximum peuvent être montées simultanément.

REMARQUE Pour restaurer des fichiers avec la restauration en mode fichier, VMware Tools doit être installé sur la machine virtuelle à partir de laquelle vous vous connectez au Restore Client. Une machine virtuelle sur laquelle VMware Tools est installé peut utiliser le Restore Client pour restaurer des fichiers à partir de sauvegardes de machines sur lesquelles VMware Tools n'était pas installé. Par contre, les machines sans VMware Tools ne peuvent pas restaurer des fichiers sauvegardés avec le Restore Client.

REMARQUE Le Restore Client ne prend pas en charge l'utilisation de VMware vSphere vMotion ou de VMware vSphere Storage vMotion.

Configurations prises en charge pour la restauration en mode fichier :

La restauration en mode fichier peut être effectuée sur des sauvegardes des systèmes de fichiers suivants :

- NTFS (partition primaire avec MBR)
- Ext2 (partition primaire avec MBR)
- Ext3 (partition primaire avec MBR)
- LVM avec ext2 (partition primaire avec MBR et une LVM autonome [sans MBR] avec ext2)
- LVM avec ext3 (partition primaire avec MBR et une LVM autonome [sans MBR] avec ext3)

Limitations de la restauration en mode fichier

La restauration en mode fichier ne prend pas en charge les configurations de disques virtuels suivantes :

- Disques non formatés
- Disques dynamiques (Windows)/Partitions multidisques (partitions composées de 2 disques virtuels ou plus)
- Disques GPT (GUID Partition Table)
- Systèmes de fichiers ext4
- Systèmes de fichiers FAT16
- Systèmes de fichiers FAT32
- Partitions étendues
- Partitions chiffrées
- Partitions compressées

La restauration en mode fichier présente également les limitations suivantes :

- Impossible de restaurer ou de parcourir des liens symboliques
- Le parcours d'un répertoire donné contenu dans une sauvegarde ou une destination de restauration est limité à un total de 5 000 fichiers ou dossiers.
- Impossible de restaurer plus de 5 000 dossiers ou fichiers dans une même opération de restauration

Les limitations suivantes s'appliquent aux volumes logiques gérés par le Logical Volume Manager :

- Un volume physique (.vmdk) doit être mappé à exactement un volume logique
- Seuls les formatages ext2 et ext3 sont pris en charge

Options d'ouverture de session

Vous pouvez vous connecter au vSphere Data Protection Restore Client de l'une des deux manières suivantes :

Le service de restauration en mode fichier est disponible uniquement sur les machines virtuelles dont les sauvegardes sont gérées par vSphere Data Protection. Cela implique que vous devrez vous connecter (via la console vCenter ou un autre type de connexion distante) à l'une des machines virtuelles sauvegardées par vSphere Data Protection pour pouvoir vous connecter au Restore Client.

Connexion de base

Pour vous connecter en mode de connexion de base, connectez-vous d'abord au Restore Client à partir d'une machine virtuelle sauvegardée par vSphere Data Protection. Vous vous connectez au Restore Client avec les informations d'identification d'administration locales de la machine virtuelle à laquelle vous êtes connecté. Le Restore Client n'affiche que les sauvegardes de la machine virtuelle à laquelle vous êtes connecté, et tous les fichiers restaurés le sont sur la machine virtuelle à laquelle vous êtes actuellement connecté.

Connexion avancée

Pour vous connecter en mode de connexion avancée, connectez-vous d'abord au Restore Client à partir d'une machine virtuelle sauvegardée par vSphere Data Protection. Vous vous connectez au Restore Client avec les informations d'identification d'administration locales de la machine virtuelle à laquelle vous êtes connecté, ainsi qu'avec celles du vCenter Server. Après vous être connecté au Restore Client, vous serez en mesure de monter, parcourir et restaurer des fichiers à partir de n'importe quelle machine virtuelle qui a été sauvegardée par vSphere Data Protection. Tous les fichiers restaurés le sont sur la machine virtuelle à laquelle vous êtes actuellement connecté.

Utiliser le Restore Client en mode de connexion de base

Utilisez le Restore Client sur une machine virtuelle Windows ou Linux en mode de connexion de base pour accéder à des fichiers à partir de points de restauration sur cette machine, au lieu de restaurer la machine virtuelle dans son intégralité.

Conditions préalables

Une sauvegarde vSphere Data Protection ne peut être effectuée que si VMware Tools est installé sur la VM (se reporter au site Web de VMware pour connaître les systèmes d'exploitation prenant en charge VMware Tools).

Les types de disque suivants sont pris en charge par le Restore Client :

- Windows (disque de base, non étendu) : NTFS
- Linux (disque de base, non étendu) : LVM, Ext 2, Ext 3

Procédure

1 Bureau distant ou utilisez un vSphere Web Client pour accéder à l'hôte local qui a été sauvegardé via vSphere Data Protection.

2 Accédez au vSphere Data Protection Restore Client via :

https://<*adresse IP de l'appliance VDP*>:8543/flr

3 À la page des informations d'identification, entrez un **nom d'utilisateur** et un **mot de passe** pour l'hôte local, puis cliquez sur **Connexion**.

4 La boîte de dialogue Gérer les sauvegardes montées s'affiche. Elle répertorie les points de restauration pour le client auquel vous accédez. Sélectionnez le point de montage qui sera restauré et cliquez sur **Monter**.

5 Une fois le montage terminé, l'icône du lecteur devient un lecteur réseau de couleur verte.

6 Cliquez sur **Fermer**.

7 Dans la fenêtre Sauvegardes montées, sélectionnez les dossiers et fichiers que vous souhaitez restaurer.

8 Cliquez sur **Restaurer les fichiers sélectionnés...**.

9 Dans la boîte de dialogue Sélectionner une destination, sélectionnez le lecteur et le dossier de destination à restaurer.

10 Cliquez sur **Restaurer**.

11 Dans la fenêtre de confirmation Démarrer la restauration qui s'ouvre, cliquez sur **Oui**.

12 Dans la boîte de dialogue La restauration a démarré qui s'ouvre, cliquez sur **OK**.

13 Cliquez sur l'onglet **Surveiller les restaurations** pour afficher l'état de la restauration.

14 Vérifiez que la procédure est terminée.

Utiliser le Restore Client en mode de connexion avancée

Utilisez le Restore Client sur une machine virtuelle Windows ou Linux en mode de connexion avancée pour accéder aux machines virtuelles d'un vCenter Server qui contiennent des points de restauration en vue d'effectuer une restauration en mode fichier.

Conditions préalables

La sauvegarde ne peut être effectuée que si VMware Tools est installé sur la VM (se reporter au site Web de VMware pour connaître les systèmes d'exploitation prenant en charge VMware Tools).

Les types de disque suivants sont pris en charge par le Restore Client.

- Windows (disque de base, non étendu) : NTFS
- Linux (disque de base, non étendu) : LVM, Ext 2, Ext 3

Procédure

1 Utilisez le Bureau à distance ou un vSphere Web Client pour accéder à une machine virtuelle.

2 Accédez au vSphere Data Protection Restore Client via :

https://*<adresse IP de l'appliance VDP>*:8543/flr

3 À la page des informations d'identification, sous Informations d'identification locales, entrez un **nom d'utilisateur** et un **mot de passe** pour l'hôte local. Dans les informations d'identification vCenter, entrez le **nom d'utilisateur** et le **mot de passe** de l'administrateur vCenter et cliquez sur **Connexion**.

4 La boîte de dialogue Gérer les sauvegardes montées s'affiche. Elle répertorie les points de restauration pour le client auquel vous accédez. Sélectionnez le point de montage qui sera restauré et cliquez sur **Monter**.

5 Une fois le montage terminé, l'icône du lecteur devient un lecteur réseau de couleur verte.

6 Cliquez sur **Fermer**.

7 Dans la fenêtre Sauvegardes montées, accédez à la machine virtuelle et sélectionnez les dossiers et les fichiers que vous souhaitez restaurer.

8 Cliquez sur **Restaurer les fichiers sélectionnés...**

9 Dans la boîte de dialogue Sélectionner une destination, sélectionnez le lecteur et le dossier de destination à restaurer.

10 Cliquez sur **Restaurer**.

11 Dans la fenêtre de confirmation Démarrer la restauration qui s'ouvre, cliquez sur **Oui**.

12 Dans la boîte de dialogue La restauration a démarré qui s'ouvre, cliquez sur **OK**.

Vous pouvez déterminer la fin de l'opération de restauration en cliquant sur l'onglet **Surveiller les restaurations** pour afficher l'état de la restauration.

Procédures d'arrêt et de démarrage de vSphere Data Protection

Si vous devez arrêter l'appliance vSphere Data Protection, utilisez l'action **Arrêt de l'OS invité**. Cette action effectue automatiquement un arrêt sans erreur de l'appliance. Si l'appliance est arrêtée sans action Arrêt de l'OS invité, des risques de détérioration existent. Une fois que l'appliance est arrêtée, elle peut être redémarrée via l'action **Mise sous tension**.

Si l'appliance ne s'arrête pas correctement, un retour arrière au dernier point de contrôle validé est effectué à son redémarrage. Cela signifie que les modifications apportées aux procédures de sauvegarde ou aux sauvegardes ayant lieu entre le point de contrôle et l'arrêt non planifié sont perdues. Ce comportement est normal et permet de s'assurer que le système n'est pas détérioré en cas d'arrêt non planifié. Pour plus d'informations, reportez-vous à la rubrique « Utilisation de points de contrôle et retour arrière » à la page 35.

IMPORTANT L'appliance vSphere Data Protection est conçue pour fonctionner 24x7 afin de prendre en charge les opérations de maintenance et de rester disponible pour des opérations de restauration. Elle ne doit pas être arrêtée sauf si une raison particulière l'exige.

Gestion de la capacité de vSphere Data Protection

4

Ce chapitre, relatif à la gestion de la capacité de vSphere Data Protection, comporte les rubriques suivantes :

Conséquences du choix de disques provisionnés fins ou épais

Le choix de partitions de disques provisionnés fins ou épais pour le datastore vSphere Data Protection présente des avantages et des inconvénients.

Le Thin Provisioning fait appel à la technologie de virtualisation pour permettre la présentation d'un nombre de ressources disque plus important que ce qui est physiquement disponible. Il peut être utilisé si un administrateur surveille activement l'espace disque et peut allouer un espace disque physique supplémentaire à mesure que le disque fin se remplit. Si l'espace n'est pas géré et que le datastore vSphere Data Protection réside sur un disque provisionné fin incapable d'allouer de l'espace, l'appliance vSphere Data Protection tombe en panne. Si tel est le cas, vous pouvez revenir en arrière vers un point de contrôle validé (voir « Utilisation de points de contrôle et retour arrière » à la page 35 pour en savoir plus). Toutes les sauvegardes qui ont lieu après le point de contrôle seront perdues.

Le Thick Provisioning alloue le stockage nécessaire lorsque le disque est créé. Pour le datastore vSphere Data Protection, la meilleure pratique consiste à créer un disque provisionné fin lorsque l'appliance vSphere Data Protection est déployée (cela permet un déploiement rapide) et, après le déploiement, à convertir le disque du Thin Provisioning en Thick Provisioning.

La procédure suivante permet de convertir le Thin Provisioning en Thick Provisioning. Cette procédure nécessite que l'appliance vSphere Data Protection soit arrêtée et peut prendre plusieurs heures.

Conditions préalables

L'appliance vSphere Data Protection doit être installée avec le Thin Provisioning. L'espace disque doit être suffisant pour augmenter la capacité du disque jusqu'au Thick Provisioning.

Procédure

1. Dans vSphere Client, cliquez avec le bouton droit de la souris sur l'appliance vSphere Data Protection et sélectionnez **Arrêt de l'OS invité**.
2. Mettez l'appliance en surbrillance et sélectionnez l'onglet **Résumé**. Dans la rubrique **Stockage**, cliquez avec le bouton droit de la souris sur le datastore et sélectionnez **Parcourir le datastore...**
3. Sur l'écran de navigation du datastore, sélectionnez votre appliance et développez le datastore associé.
4. Cliquez avec le bouton droit de la souris sur un fichier .vmdk et sélectionnez **Augmenter**.
5. Répétez cette étape pour chaque fichier .vmdk.
   - Pour une VDP de 0,5 To, il y a trois fichiers .vmdk.
   - Pour une VDP de 1 To, il y a sept fichiers .vmdk.
   - Pour une VDP de 2 To, il y a treize fichiers .vmdk.

Incidence de la capacité de stockage pour le déploiement initial de vSphere Data Protection

Lorsqu'une nouvelle appliance vSphere Data Protection est déployée, elle se remplit rapidement les premières semaines. En effet, quasiment chaque client sauvegardé contient des données uniques. La déduplication vSphere Data Protection est plus intéressante lorsque d'autres clients similaires ont été sauvegardés ou que les mêmes clients ont été sauvegardés au moins une fois.

Après la sauvegarde initiale, l'appliance sauvegarde moins de données uniques au cours des sauvegardes suivantes. Lorsque les sauvegardes initiales sont terminées et que les périodes de rétention sont dépassées, il est possible d'envisager et de mesurer la capacité du système à stocker chaque jour quasiment autant de nouvelles données que celles dont il se libère au cours des fenêtres de maintenance.

C'est ce que l'on appelle l'utilisation de la capacité de stabilisation. La capacité de stabilisation idéale doit être de 80 %.

Surveillance de la capacité de vSphere Data Protection

Il convient de surveiller proactivement la capacité de vSphere Data Protection. Pour ce faire, consultez la capacité utilisée sous l'onglet Rapports de vSphere Data Protection.

Seuils de capacité de vSphere Data Protection

Le tableau suivant décrit le comportement de vSphere Data Protection pour des seuils de capacité clés :

Tableau 4-1. Seuils de capacité de vSphere Data Protection

Seuil	Valeur	Comportement
Avertissement de capacité	80 %	vSphere Data Protection génère un événement d'avertissement.
Limite de contrôle d'intégrité	95 %	Les sauvegardes en cours peuvent se terminer, mais les nouvelles activités de sauvegarde sont suspendues. vSphere Data Protection génère des événements d'avertissement.
Limite de serveur en lecture seule	100 %	vSphere Data Protection passe en mode de lecture seule, et aucune nouvelle donnée n'est autorisée.

Gestion de la capacité

Lorsque vous dépassez une capacité de 80 %, suivez les conseils ci-dessous pour gérer la capacité :

- Arrêtez d'ajouter des VM comme clients de sauvegarde
- Supprimez les procédures de sauvegarde inutiles
- Réévaluez les règles de rétention pour déterminer si vous pouvez l'alléger
- Envisagez l'ajout d'appliances vSphere Data Protection pour répartir les procédures de sauvegarde entre plusieurs appliances

Dépannage de vSphere Data Protection

5

Ce chapitre contient les rubriques de dépannage suivantes :

Installation de l'appliance vSphere Data Protection

Si vous rencontrez des difficultés lors de l'installation de l'appliance vSphere Data Protection :

- Vérifiez que tous les logiciels répondent à la configuration logicielle minimale requise (voir « Configuration logicielle » à la page 13).
- Vérifiez que l'ensemble du matériel répond à la configuration matérielle minimale requise (voir « Configuration matérielle » à la page 13).
- Vérifiez que le serveur DNS est correctement configuré pour l'appliance vSphere Data Protection. (Voir « Configuration préalable à l'installation » à la page 14)

Sauvegardes vSphere Data Protection

Les problèmes recensés concernant les sauvegardes vSphere Data Protection sont les suivants :

« Chargement en cours des données de la procédure de sauvegarde... »

Ce message peut apparaître durant quelques minutes (5 au maximum) lorsqu'un grand nombre de VM (environ une centaine) sont sélectionnées pour une seule procédure de sauvegarde. Ce problème peut également s'appliquer à des actions de verrouillage/déverrouillage, d'actualisation ou de suppression pour les procédures volumineuses. Ce comportement est normal lorsque des procédures très volumineuses sont sélectionnées. Ce message disparaît une fois l'action terminée, après un délai de 5 minutes au maximum.

« Impossible d'ajouter le client {nom du client} à l'appliance VDP lors de la création ou modification de la procédure de sauvegarde {nom de la procédure de sauvegarde}. »

Cette erreur peut se produire s'il existe un doublon du nom du client sur le conteneur vApp ou sur l'hôte VMware ESX/ESXi. Dans ce cas, une seule procédure de sauvegarde est ajoutée. Résolvez les doublons de nom de client.

« Les éléments suivants sont introuvables et n'ont pas été sélectionnés :{nom du client}. »

Cette erreur peut se produire lors de la modification d'une procédure de sauvegarde, lorsque les VM sauvegardées sont introuvables. Ce problème a déjà été recensé.

Il arrive que les VM Windows 2008 R2 ne peuvent pas sauvegarder si “disk.EnableUUID” est configuré sur « true ».

Les sauvegardes Windows 2008 R2 peuvent échouer si les VM sont configurées avec *disk.EnableUUID* défini sur *true*. Pour corriger ce problème, vous pouvez mettre à jour manuellement le paramètre de configuration vmx *disk.EnableUUID* sur *false*.

Pour configurer *disk.EnableUUID* sur *false* à l'aide du vSphere Web Client :

1. Arrêtez la VM en cliquant dessus avec le bouton droit de la souris et en sélectionnant **Arrêt de l'OS invité**.
2. Cliquez avec le bouton droit de la souris sur la VM et sélectionnez **Modifier les paramètres**.
3. Cliquez sur **Options VM**.
4. Développez la rubrique **Avancé** et cliquez sur **Modifier la configuration**.
5. Localisez le nom *disk.EnableUUId* et définissez la valeur sur *false*.
6. Cliquez sur **OK**.
7. Cliquez sur **OK**.
8. Cliquez avec le bouton droit de la souris sur la VM et sélectionnez **Mise sous tension**.

Après la mise à jour du paramètre de configuration, les sauvegardes de la VM Windows 2008 R2 devraient réussir.

La sauvegarde échoue si la capacité du datastore de vSphere Data Protection est insuffisante.

Les sauvegardes planifiées échouent à 92 % si la capacité du datastore de vSphere Data Protection est insuffisante. Si le datastore de vSphere Data Protection est configuré avec le Thin Provisioning et que la capacité maximale n'est pas atteinte, ajoutez des ressources de stockage supplémentaires. Si le datastore de vSphere Data Protection est configuré avec le Thick Provisioning et a atteint sa capacité maximale, reportez-vous à la rubrique « Gestion de la capacité de vSphere Data Protection » à la page 41.

La sauvegarde échoue si une VM est activée avec VMware Fault Tolerance.

Si la tolérance aux pannes est activée sur une VM, la sauvegarde échoue. Ce comportement est normal puisque vSphere Data Protection ne prend pas en charge la sauvegarde de VM dont la tolérance aux pannes est activée.

Lorsque les VM rejoignent ou quittent différents groupes de cluster, il arrive que les sources de sauvegarde associées soient perdues.

Lorsque les hôtes rejoignent des clusters avec l'option de conserver les pools de ressources et les vApps, les conteneurs sont recréés, et non pas copiés. Par conséquent, il ne s'agit plus du même conteneur même si son nom reste inchangé. Validez ou recréez les procédures de sauvegarde qui protègent des conteneurs après que les hôtes ont rejoint ou quitté un cluster.

Suite à un arrêt non planifié, les procédures de sauvegarde et les sauvegardes récentes sont perdues.

Chaque fois qu'un arrêt non planifié se produit, l'appliance vSphere Data Protection revient en arrière au dernier point de contrôle validé. Ce comportement est normal. Pour plus d'informations, reportez-vous à « Utilisation de points de contrôle et retour arrière » à la page 35.

Restaurations de vSphere Data Protection

Les problèmes recensés relatifs aux restaurations vSphere Data Protection sont les suivants :

L'onglet Restauration affiche un message de chargement des sauvegardes en cours, et le chargement est lent.

En principe, le chargement d'une sauvegarde VM à partir de l'onglet Restauration prend deux secondes. Ce comportement est normal.

La restauration échoue à l'emplacement d'origine si la VM est associée à des snapshots.

Si une VM est associée à des snapshots, la restauration à l'emplacement d'origine échoue. Ce comportement est normal puisque vSphere Data Protection ne prend pas en charge la restauration de VM associées à des snapshots sur l'emplacement d'origine. Restaurez la VM à un autre emplacement ou supprimez les snapshots avant d'effectuer la restauration à l'emplacement d'origine.

Restauration en mode fichier

Les problèmes recensés pour la restauration en mode fichier avec le vSphere Data Protection Restore Client sont les suivants :

Lors d'un montage de restauration en mode fichier, seule la dernière partition s'affiche si le fichier VMDK contient plusieurs partitions.

Le Restore Client ne prend pas en charge les volumes étendus. Ce comportement est normal. Effectuez une restauration en mode image et copiez manuellement les fichiers nécessaires.

Lors d'un montage de restauration en mode fichier, les partitions non prises en charge ne peuvent pas être montées.

Les formats de disque suivants n'étant pas pris en charge par le Restore Client, l'échec de son montage est un comportement normal.

- Disque non formaté
- FAT32
- Partitions étendues
- Disques dynamiques
- Disques GPT
- Système de fichiers ext4
- Partitions chiffrées
- Partitions compressées

Effectuez une restauration en mode image et copiez manuellement les fichiers nécessaires.

Les liens symboliques ne sont pas affichés dans le Restore Client.

Le Restore Client ne prend pas en charge l'affichage de liens symboliques.

Reporting vSphere Data Protection

Les problèmes recensés concernant le reporting vSphere Data Protection sont les suivants :

L'onglet Restauration est lent à se charger ou à s'actualiser.

Si le nombre de VM est important, l'onglet Restauration met du temps à se charger ou à s'actualiser. Au cours de tests avec 100 VM, le chargement a pris environ quatre minutes et demie.

Utilisation des ports par vSphere Data Protection

6

vSphere Data Protection utilise les ports répertoriés dans le tableau suivant.

Tableau 6-1. Utilisation des ports par vSphere Data Protection

Port	Protocole(s)	Service associé
22	TCP	ssh
80	TCP	http
111	TCP	rpcbind
443	TCP	https
700	TCP	Outil Loginmgr
5555	TCP	Postgres
5558	TCP	Postgres
7778	TCP	RMI VDP
7779	TCP	RMI VDP
8509	TCP	Connecteur Tomcat AJP
8543	TCP	Redirection pour Tomcat
8580	TCP	VDP Downloader
9443	TCP	Services Web VDP
25000	TCP/UDP	Communications internes VDP
26000	TCP/UDP	Communications internes VDP
27000	TCP	Communications client-serveur VDP
28001	TCP	Proxy interne de VDP
28002	TCP	Proxy interne de VDP
28003	TCP	Proxy interne de VDP
28004	TCP	Proxy interne de VDP
28005	TCP	Proxy interne de VDP
28006	TCP	Proxy interne de VDP
28007	TCP	Proxy interne de VDP
28008	TCP	Proxy interne de VDP
28009	TCP	Proxy interne de VDP
29000	TCP	Communications client internes sécurisées de VDP
34250	TCP	ssl/soap gSoap (hôte local)
53	UDP	DNS

Tableau 6-1. Utilisation des ports par vSphere Data Protection

Port	Protocole(s)	Service associé
111	UDP	RPC
941	UDP	RPC

Reprise après sinistre de vSphere Data Protection 7

vSphere Data Protection offre de puissantes fonctions de stockage et de gestion des sauvegardes. En cas de panne, la première mesure à prendre consiste à revenir en arrière vers un point de contrôle validé (voir « Utilisation de points de contrôle et retour arrière » à la page 35). Pour la reprise d'une appliance vSphere Data Protection en cas de panne, suivez la procédure ci-après pour créer des sauvegardes de l'appliance et de toutes les sauvegardes vSphere Data Protection associées.

Procédure de reprise après sinistre vSphere Data Protection :

1. Avant d'arrêter l'appliance vSphere Data Protection, vérifiez qu'aucune procédure de sauvegarde ou de maintenance n'est en cours. Selon la méthode de sauvegarde choisie et la durée de l'opération, planifiez votre sauvegarde vSphere Data Protection à un moment où aucune autre tâche n'est planifiée.
   Par exemple, si votre fenêtre de sauvegarde est de huit heures et que vos sauvegardes ne prennent qu'une heure, vous disposez de sept heures supplémentaires avant le démarrage de tâches de maintenance. C'est le meilleur moment d'arrêter l'appliance et de la sauvegarder. Pour plus d'informations, reportez-vous à « Configuration de la fenêtre de sauvegarde » à la page 32.
2. Dans le vSphere Client, accédez à l'appliance. Effectuez un arrêt de l'OS invité sur la machine virtuelle. N'éteignez pas la machine virtuelle à partir de son interface. Une tâche de « mise hors tension » équivaut à débrancher l'alimentation du serveur physique et risque d'entraîner un arrêt avec des erreurs. Pour plus d'informations, reportez-vous à « Procédures d'arrêt et de démarrage de vSphere Data Protection » à la page 39.
3. Une fois que vous avez vérifié l'arrêt de l'appliance, poursuivez avec votre méthode de protection privilégiée.
4. Vérifiez que la sauvegarde de vSphere Data Protection est terminée et qu'aucune procédure de sauvegarde/snapshot/copie n'est en cours pour vSphere Data Protection.
5. Dans le vSphere Client, effectuez une mise sous tension de l'appliance.

Index

U

V

Z